UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	04/04/2023	11620621	124452.00122	2047

27557 7590 03/15/2023

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 70 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

Robert Evan POLLIN, Rockville, MD;
Brian Edward DOWNEY JR., Alexandria, VA;
Sean Allen FLEMING, Germantown, MD;

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Autoscribe Corporation, Gaitherburg, MD;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Nuvei Techs., Inc.
EX1002
Page 1 of 442

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

27557 7590 02/22/2023

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER
AZIZ, ABDULMAJEED

ART UNIT	PAPER NUMBER
3695	

DATE MAILED: 02/22/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

TITLE OF INVENTION: Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/22/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27557 7590 02/22/2023

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

TITLE OF INVENTION: Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/22/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
AZIZ, ABDULMAJEED	3695	705-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

27557 7590 02/22/2023

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER	
AZIZ, ABDULMAJEED	
ART UNIT	**PAPER NUMBER**
3695	

DATE MAILED: 02/22/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/535,424	Applicant(s) POLLIN et al.	
	Examiner ABDULMAJEED AZIZ	Art Unit 3695	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to the amendment submitted on 1/5/23.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-4,7,12-13,16-19,22,27-28,31-33,35,38,40-42 and 46-50 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ABDULMAJEED AZIZ/
Primary Examiner, Art Unit 3695

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

2. **Claims 1-4, 7, 12-13, 16-19, 22, 27-28, 31-33, 35, 38, 40-42 & 46-50** (**the claimed invention**) are allowed.

3. A **Terminal Disclaimer** has been filed for US 10423940 & US 9576279 on 2/3/23.

Reasons for Patent Eligibility under 35 USC §101

4. **The claimed invention** overcomes 101. Applicant's arguments regarding 101 filed in the response on **1/5/23** were fully considered, along with the Examiner's amendment, and are persuasive in light of the 2019 Patent Eligibility Guidance (PEG). Related to the analysis:

Step 1: The claims are directed to a method or system? YES

Step 2A-PRONG 1: The limitations of **Claim 1** (additional elements are emphasized in **bold** and to be removed to identify the abstract idea)**:**

---

1. (Currently Amended): A method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers, the method comprising:

providing**, by the one or more secure servers to a merchant server providing a webpage to a payer computing system** used by the payer, **an application programming interface (API)** that:

provides financial account registration and token retrieval functions that can be executed to process the payment transaction;

provides access to the financial account registration and token retrieval functions to **the merchant server**;

receives**, from the merchant server via the API,** at least one data element associated with the payer and a payment amount from the payer to the payee;

authenticates the payee; and

executes the financial account registration function, upon initiation by the **merchant server**, by:

generating a **uniform resource locator (URL)**, for establishing **a secure socket layer connection via the internet between the secure server and the payer computing system**, the **URL** comprising either:

a dynamic **URL** generated by the **secure server** for the payer and the payee; or

a static **URL** and **a hypertext transport protocol (HTTP) parameter used by the secure server** to identify the payer and the payee;

establishing **the secure socket layer connection**, in response to an **HTTP request** received from the **merchant server** for the generated **URL**, between the **secure server and the payer computing system within a window or frame that is displayed within the webpage** provided by the **merchant server**;

outputting instructions to the **payer computing system**, in response to the **HTTP request** for the generated **URL**, to render a financial account registration request form, within the **window or frame that is displayed within the webpage provided by the merchant server**, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

outputting instructions to the payer computing system, in response to the **HTTP request** for the generated **URL**, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the **secure server via the secure socket layer connection**;

receiving the sensitive financial account information provided by the payer via the **secure socket layer connection**;

storing the sensitive financial account information in a secure storage location and performing each **software** process required to maintain compliance with one or more information security standards;

executing a token retrieval function**, upon initiation by the merchant server via the API,** by:

providing a non-sensitive electronic data token representing the sensitive financial account information to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and

processing the payment transaction using the sensitive financial account information by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

---

includes a process that under its broadest reasonable interpretation, covers performance of the limitation as a **Certain method of organizing human activity (fundamental economic practice** or **commercial or legal interaction**) of **processing a payment from a payer to a payee**.. YES, the claims are abstract.

Step 2A-PRONG 2: Is the judicial exception integrated into a practical application? The limitations, identified at least by the additional elements in the above analysis, are indicative of integration into a practical application. The limitations are an improvement to computing security.

Arguments presented on 1/5/23 (p. 8-9), provide further nexus to integration into a practical application:

> [p. 22-23] "technical challenges of complying with data security standards (such as the PCI standard attached as Appendix A) …thereby reducing the time and cost of developing the merchant server 204: [0028] ... Using the methods disclosed herein, in preferred embodiments merchants are able to process such transactions without transmitting, processing or storing Financial Account data. This **reduces the potential liability of the merchants for data loss, and avoids placing their customer tracking and payment processing systems (such as merchant server 204) within the scope of the present Payment Card Industry Data Security Standard (PCI-DSS)**, thus reducing compliance costs, development costs, and accelerating time-to-market."

> [p. 23] "The claimed invention improves the functioning of the prior art merchant server itself by **eliminating the need for the merchant server to "store financial account information in a secure storage location and perform each software process required to maintain compliance with one or more information security standards**" By eliminating the need for merchant servers to receive, store, and transmit financial account information, the claimed invention eliminates the need for those merchant servers to include the hardware components and perform the software processes required to maintain compliance with information security standards, like **the PCI Data**

Security Standard that was in place on the effective filing date of the present application[42] that is attached as Appendix A."

[p. 27-28] "By providing a financial account registration request form to payers of multiple merchants via an application programming interface (for example, within windows or frames that are displayed within the webpages provided by those merchant servers), the secure server can provide a single interface that masks that PAN when displayed,[77] a single process to remove stored cardholder data exceeding the requirements defined in the secure system's data retention policy,[78] and a single process to securely delete sensitive authentication data.[79] The secure system can protect that cardholder data for all of those merchant systems by generating strong data-encrypting cryptographic keys, encrypting those data-encrypting cryptographic keys using key-encrypting cryptographic keys, securely storing the cryptographic keys, and retiring or replacing the cryptographic keys when required.[80] One particularly beneficial improvement provided by the claimed invention is the secure system can perform a single key rotation process and ensure that all cryptographic keys used for all merchants are changed before they reach the end of their cryptoperiod."

Therefore, the claimed invention is eligible under step 2a prong 2.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given via email correspondence based on an interview with **Jonathan King** (Applicant's representative) on **1/9/23**.

The application has been amended as follows:

Claims:

1. (Currently Amended): A method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers, the method comprising:

providing, by the one or more secure servers to a merchant server providing a webpage to a payer computing system used by the payer, an application programming interface (API) that:

~~provides an API endpoint that receives an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including~~

provides financial account registration and token retrieval functions that can be executed to process the payment transaction;

provides access to the financial account registration and token retrieval functions to the merchant server;

receives, from the merchant server via the API, at least one data element associated with the payer and ~~specifying the amount of the payment~~ a payment amount from the payer to the payee;

authenticates the payee; and

executes the financial account registration function, upon initiation by the merchant server, by:

~~generates a universal~~ generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

~~establishes~~ establishing the secure socket layer connection, in response to an HTTP request received from the merchant server for the generated URL, between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

~~outputs~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

~~outputs~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server[[,]] via the secure socket layer connection~~, without providing the financial account information to the merchant server~~;

receiving the sensitive financial account information provided by the payer via the secure socket layer connection;

storing the sensitive financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

executing a token retrieval function, upon initiation by the merchant server via the API, by:

providing [[an]] a non-sensitive electronic data token[[,]] representing the sensitive financial account information ~~provided by the payer,~~ to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and

processing the payment transaction using the sensitive financial account information ~~provided by the payer; and~~ by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

2. (Currently Amended): The method of claim 1, further comprising:

receiving a second payment transaction instruction from the merchant server, the second payment transaction instruction including a representation of the non-sensitive electronic data token and specifying a second payment amount ~~the amount of the second payment from the payer to the payee~~;

processing the second payment by obtaining the second payment amount using the sensitive financial account information represented by the non-sensitive electronic data token; and

forwarding at least a portion of the second payment amount to the payee.

3. (Currently Amended): The method of claim 2, wherein the representation of the non-sensitive electronic data token is the non-sensitive electronic data token.

4. (Currently Amended): The method of claim 1, wherein the ~~payment transaction instruction is generated by the merchant server using the application programming interface provided by the secure server~~ non-sensitive electronic data token constitutes a symbolic representation of the sensitive financial account information.

5. (Cancelled)

7. (Currently Amended): The method of ~~claim 4~~ claim 1, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

12. (Currently Amended): The method of claim 1, wherein the secure socket layer connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data provided by the payer.

13. (Currently Amended): The method of claim 1, wherein the sensitive financial account information includes at least one of a credit card number or bank account number.

14. - 15. (Cancelled)

16. (Currently Amended): A secure server that processes a payment transaction from a payer to a payee, the secure server comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the secure server to:

provide an application programming interface (API) to a merchant server providing a webpage to a payer computing system used by the payer, the API configured to:

~~provide an API endpoint configured to receive an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including~~

provide financial account registration and token retrieval functions that can be executed to process the payment transaction;

provide access to the financial account registration and token retrieval functions to the merchant server;

receive, from the merchant server via the API, at least one data element associated with the payer and ~~specifying an amount of the payment~~ a payment amount from the payer to the payee;

authenticate the payee;

execute the financial account registration function, upon initiation by the merchant server, by:

~~generate a universal~~ generating a uniform resource locator (URL) to establish a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

~~establish~~ establishing the secure socket layer connection, in response to an HTTP request received from the merchant server for the generated URL, between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

~~output~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

~~output~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server[[,]] via the secure socket layer connection~~, without providing the financial account information to the merchant server~~;

receive the sensitive financial account information provided by the payer via the secure socket layer connection;

store the sensitive financial account information in a secure storage location and perform each software process required to maintain compliance with one or more information security standards;

execute a token retrieval function, upon initiation by the merchant server by the API, by:

~~provide an~~ providing a non-sensitive electronic data token[[,]] representing the sensitive financial account information ~~provided by the payer,~~ to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and

~~store the financial account information provided by the payer;~~

processing the payment transaction using sensitive the financial account information ~~provided by the payer; and~~ by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

17. (Currently Amended): The secure server of claim 16, wherein the instructions further cause the secure computing system to:

receive a second payment transaction instruction from the merchant server, wherein the second payment transaction instruction includes a representation of the non-sensitive electronic data token and specifies ~~an amount of~~ a second payment amount ~~from the payer to the payee~~;

process the second payment by obtaining the second payment amount using the sensitive financial account information represented by the non-sensitive electronic data token; and

forward at least a portion of the second payment amount to the payee.

18. (Currently Amended): The secure server of claim 17, wherein the representation of the non-sensitive electronic data token is the non-sensitive electronic data token.

19. (Currently Amended): The secure server of claim 16, wherein the ~~payment transaction instruction is generated by the merchant server using the application programming interface provided by the secure server~~ non-sensitive electronic data token constitutes a symbolic representation of the sensitive financial account information.

20. (Cancelled)

22. (Currently Amended): The secure server of ~~claim 19~~ claim 16, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

27. (Currently Amended): The secure server of claim 16, wherein the secure socket layer connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

28. (Currently Amended): The secure server of claim 16, wherein the sensitive financial account information includes at least one of a credit card number or bank account number.

29. - 30. (Cancelled)

31. (Currently Amended): A method of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising:

providing a webpage to a payer computing system used by a payer;

receiving enrollment data identifying ~~a payer~~ the payer;

~~generating an electronic instruction for a secure server that includes~~ providing, to a secure server via an application programming interface (API) provided by the secure server, at least one data element associated with the payer~~, the electronic instruction requesting the establishment of~~ and a payment amount from the payer to the payee;

displaying a window or frame within the webpage provided to the payer computing system;

providing authentication credentials to the API to establish an authenticated session, the authentication credentials identifying the payee and authenticating the payee;

initiating a financial account registration function of the API during the authenticated session, the financial account registration function:

establishing a secure socket layer connection ~~via the internet~~ between the secure server and the payer computing system within the window or frame~~a computing system used by the payer for the secure server to receive financial account information provided by the payer~~;

~~outputting the electronic instruction to a communications network for transmittal to the secure server;~~

outputting instructions to the payer computing system to render a financial account registration request form, within the window or frame, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

outputting instructions to the payer computing system to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server, via the secure socket layer connection, without providing the sensitive financial account information to the merchant server;

~~receiving, from the secure server, an~~ initiating a token retrieval function of the API during the authenticated session, the token retrieval function outputting a non-sensitive electronic data token representing the sensitive financial account information ~~received by the secure server via the secure connection~~ to the merchant server;

receiving the non-sensitive electronic data token from the secure server, wherein the merchant server does not receive the sensitive financial account information represented by the non-sensitive electronic data token and the secure server does not provide the non-sensitive electronic data token to the payer;

storing the non-sensitive electronic data token in association with the enrollment data identifying the payer; and

processing a payment from the payer by ~~electronically~~ generating a payment transaction instruction, using the token retrieval function of the API, that includes a representation of the non-sensitive electronic data token and instructs ~~a payment processing system having access to the financial account information represented by the electronic data~~

~~token~~ the secure server to generate and transmit an electronic request requesting the payment amount from the financial account, obtain the payment amount, and forward at least a portion of the payment amount.

32. (Currently Amended): The method of claim 31, wherein the representation of the non-sensitive electronic data token is the non-sensitive electronic data token.

33. (Currently Amended): The method of claim 31, wherein ~~the electronic instruction is generated using an application programming interface provided to the merchant server by the secure server~~ the non-sensitive electronic data token constitutes a symbolic representation of the sensitive financial account information.

34. (Cancelled)

35. (Currently Amended): The method of ~~claim 33~~ claim 31, wherein the at least one data element associated with the payer is a customer identifier generated by the merchant server to identify the payer.

37. (Cancelled)

38. (Currently Amended): The method of claim 31, wherein the secure socket layer connection provides access to the secure server using a static or dynamic ~~universal~~ uniform resource locator (URL).

39. (Cancelled)

40. (Currently Amended): The method of claim 31, wherein the secure socket layer connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

42. (Currently Amended): The method of claim 31, wherein the sensitive financial account information includes at least one of a credit card number or bank account number.

43. - 45. (Cancelled)

46. (Currently Amended): A merchant server, operated by or for the benefit of a payee, comprising:

one or more computer processors; and

non-transitory computer readable storage media storing instructions that, when executed by the one or more computer processors, cause the merchant server to:

provide a webpage to a payer computing system used by a payer;

receive enrollment data identifying ~~a~~the payer;

~~generate an electronic instruction for a secure server that includes~~ provide, to a secure server via an application programming interface (API) provided by the secure server, at least one data element associated with the payer~~, the electronic instruction requesting the establishment of~~ and a payment amount from the payer to the payee;

display a window or frame within the webpage provided to the payer computing system;

provide authentication credentials to the API to establish an authenticated session, the authentication credentials identifying the payee and authenticating the payee;

initiate a financial account registration function of the API during the authenticated session, the financial account registration function:

establishing a secure socket layer connection ~~via the internet~~ between the secure server and [[a]] the payer computing system ~~used by the payer for the secure server to receive financial account information provided by the payer~~ within the window or frame;

~~output the electronic instruction to a communications network for transmittal to the secure server;~~

outputting instructions to the payer computing system to render a financial account registration request form, within the window or frame, that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

outputting instructions to the payer computing system to encrypt the sensitive financial account information provided by the payer and transmit the encrypted financial account information to the secure server via the secure socket layer connection;

~~receive, from the secure server, an~~ initiate a token retrieval function of the API during the authenticated session, the token retrieval function outputting a non-sensitive electronic data token representing the sensitive financial account information ~~received by the secure server provided by the payer via the communications link~~ to the merchant server;

receive the non-sensitive electronic data token from the secure server, wherein the merchant server does not receive the sensitive financial account information represented by the non-sensitive electronic data token and the secure server does not provide the non-sensitive electronic data token to the payer;

store the non-sensitive electronic data token in association with the enrollment data identifying the payer; and

process a payment from the payer by ~~electronically~~ generating a payment transaction instruction, using the token retrieval function of the API, that includes a representation of the non-sensitive electronic data token and ~~electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token~~ instructs the secure server to generate and transmit an electronic request requesting the payment amount from the financial account, obtain the payment amount, and forward at least a portion of the payment amount.

47. (Currently Amended): The merchant server of claim 46, wherein ~~secure connection is a window or frame within a website provided by the merchant server~~ the non-sensitive electronic data token constitutes a symbolic representation of the sensitive financial account information.

48. (Currently Amended): A method of processing a payment transaction from a payer to a payee, the method being performed by one or more secure servers, the method comprising:

providing, by the one or more secure servers to a merchant server providing a webpage to a payer computing system used by the payer, an application programming interface (API) that:

~~provides an API endpoint that receives an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including~~

provides financial account registration and token retrieval functions that can be executed to process the payment transaction;

provides access to the financial account registration and token retrieval functions to the merchant server;

receives, from the merchant server via the API, at least one data element associated with the payer and ~~specifying the amount of the payment~~ a payment amount from the payer to the payee;

authenticates the payee; and

executes the financial account registration function, upon initiation by the merchant server, by:

~~generates a universal~~ generating a uniform resource locator (URL), for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

~~establishes~~ establishing the secure socket layer connection, in response to an HTTP request received for the generated URL, between the secure server and the payer computing system ~~within a window or frame that is displayed within the webpage provided by the merchant server~~;

~~outputs~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to render a financial account registration request form ~~within the window or frame that is displayed within the webpage provided by the merchant server,~~ that provides functionality for the payer to provide sensitive financial account information associated with a financial account; and

~~outputs~~ outputting instructions to the payer computing system, in response to the HTTP request for the generated URL, to encrypt the financial account information provided by the payer and transmit the encrypted financial account information to the secure server, via the secure socket layer connection ~~without providing the financial account information to the merchant server~~;

receiving the sensitive financial account information provided by the payer via the secure socket layer connection;

storing the sensitive financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

executing a token retrieval function, upon initiation by the merchant server via the API, by:

providing [[an]] a non-sensitive electronic data token[[,]] representing the sensitive financial account information ~~provided by the payer,~~ to the merchant server without providing the sensitive financial account information to the merchant server and without providing the non-sensitive electronic data token to the payer; and

processing the payment transaction using the sensitive financial account information ~~provided by the payer; and~~ by generating and transmitting an electronic request requesting the payment amount from the financial account, obtaining the payment amount, and forwarding at least a portion of the payment amount to the payee.

50. (New): The method of claim 48, wherein the non-sensitive electronic data token constitutes a symbolic representation of the sensitive financial account information.

REASONS FOR ALLOWANCE

6. The following is an examiner' s statement of reasons for allowance: the prior art fails to teach or suggest the limitations of **the claimed invention.**

The claimed invention is non-obvious as nothing in the prior art of record would suggest that the references would be combined the way they are set forth in the rejection to teach the claimed invention without knowledge of the applicant' s disclosure.

Most Relevant Prior Art:

Soman (US 20120005038) provides a system and method for PCI-compliant transactions.

Tieken (US 20110161233) provides a method for providing secure transactions that include receiving an identifier of a financial account at a payment processor system (secure server).

Basu (US 9342832) provides a method for securing external systems with account token substitution.

Therefore, **the claimed invention** has been deemed to be allowable over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record, and not relied upon, considered pertinent to applicant' s disclosure or directed to the state of art is listed on the enclosed PTO-892.

8. The following is a brief description for relevant prior art that was cited but not applied:

Hammad (US 20120259782) provides a method for authenticating a cardholder using multiple tokenization authentication.

Hammad (US 20120136796) provides a method of enrolling a mobile device in a program that provides the mobile device with the ability to conduct card-present transactions.

First Data (NPL) discusses how the TransArmor solution can enable scope reduction and ease the burden of PCI compliance.

Stringfellow (US 20120030066) provides a payment system that processes payment authorization requests for payment transactions to be conducted via a data communications network on behalf of online merchants, and is particularly, but not exclusively, suited to the processing of orders placed by financial instrument holders.

Moore (US 20100235286) provides a method and system for generating tokens in a transaction handling system.

Yanni (US 20040098350) provides a framework and system for purchasing of goods and services.

Franklin (US 5883810) provides an electronic online commerce card with transaction proxy number for online transactions.

Fleishman (US 20040148252) provides a person-to-person (P2P) payment platform and identity management system which facilitates online banking by allowing consumers to send and receive money in real-time, with no special registration outside of the users' existing banking relationship, and under the security, brand and control of their own respective banks.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULMAJEED AZIZ whose telephone number is (571)270-5046. The examiner can normally be reached on M-F 7-4:00 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan Donlon can be reached on 571-270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABDULMAJEED AZIZ/

Primary Examiner, Art Unit 3695

Applicant-Initiated Interview Summary	**Application No.** 16/535,424	**Applicant(s)** POLLIN et al.		
	Examiner ABDULMAJEED AZIZ	**Art Unit** 3695	**AIA (First Inventor to File) Status** No	**Page** 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
ABDULMAJEED AZIZ	Primary Examiner	Telephonic
Jonathan King	Attorney of Record	

Date of Interview: 09 January 2023

Issues Discussed:

35 U.S.C. 101

Examiner and Applicant negotiated agreement on 101 per the Examiner's amendment.

☑ Attachment

/ABDULMAJEED AZIZ/ Primary Examiner, Art Unit 3695	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN et al.
	Examiner	Art Unit
	ABDULMAJEED AZIZ	3695

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q20/10	03/12/2021	PM
G06Q20/10; G06Q10/107; G06Q20/102; G06Q20/12; G06Q20/305; G06Q20/40; G06Q20/4014; G06Q10/00	11/26/2021	PM
(G06Q20/10 OR G06Q10/107 OR G06Q20/102 OR G06Q20/12 OR G06Q20/305 OR G06Q20/40 OR G06Q20/4014 OR G06Q10/00) - limited by text	09/28/2022	aa
(G06Q20/10 OR G06Q10/107 OR G06Q20/102 OR G06Q20/12 OR G06Q20/305 OR G06Q20/40 OR G06Q20/4014 OR G06Q10/00).cpc . -limited by text	02/10/2023	aa

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/ABDULMAJEED AZIZ/ Primary Examiner, Art Unit 3695	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN et al.
	Examiner	**Art Unit**
	ABDULMAJEED AZIZ	3695

Search Notes		
Search Notes	**Date**	**Examiner**
G06Q20/10	03/12/2021	PM
East Text Search	03/12/2021	PM
Dialog NPL search	03/12/2021	PM
G06Q20/10; G06Q10/107; G06Q20/102; G06Q20/12; G06Q20/305; G06Q20/40; G06Q20/4014; G06Q10/00	11/26/2021	PM
Updated "Search" text search	11/26/2021	PM
Updated Dialog NPL search	11/26/2021	PM
Inventor/assignee, text/npl/foreign, bf-citation	09/28/2022	aa
Inventor/assignee, text/npl/foreign, bf-citation	02/10/2023	aa

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06Q	20/00	02/10/2023	aa

/ABDULMAJEED AZIZ/ Primary Examiner, Art Unit 3695	

Bibliographic Data

Application No: 16/535,424

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /ABDULMAJEED AZIZ/ Examiner's Signature | Initials

Title: Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
08/08/2019	705	3695	124452.00122
RULE			

APPLICANTS

Autoscribe Corporation, Gaitherburg, MD,

INVENTORS

Robert Evan POLLIN, Rockville, MD, UNITED STATES

Brian Edward DOWNEY JR., Alexandria, VA, UNITED STATES

Sean Allen FLEMING, Germantown, MD, UNITED STATES

CONTINUING DATA

This application is a CON of 15408185 01/17/2017 PAT 10423940

15408185 is a CON of 13679545 11/16/2012 PAT 9576279

13679545 has PRO of 61698574 09/08/2012

13679545 has PRO of 61655482 06/05/2012

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/19/2019

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403
UNITED STATES

FILING FEE RECEIVED

$1,035

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	16535424
Filing Date	08-Aug-2019
First Named Inventor	Robert POLLIN
Attorney Docket Number	124452.00122
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
AUTOSCRIBE CORPORATION	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

10423940

9576279

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 65967

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Jonathan R. King/
Name	Jonathan R. King

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	16535424
Filing Date:	08-Aug-2019
Title of Invention:	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System
First Named Inventor/Applicant Name:	Robert Evan POLLIN
Filer:	Jonathan R. King/Crystal Corsey
Attorney Docket Number:	124452.00122

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	170	170
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**170**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 16535424

Filing Date: 08-Aug-2019

Applicant/Patent under Reexamination: POLLIN

Electronic Terminal Disclaimer filed on February 3, 2023

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	47477031
Application Number:	16535424
International Application Number:	
Confirmation Number:	2047
Title of Invention:	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System
First Named Inventor/Applicant Name:	Robert Evan POLLIN
Customer Number:	27557
Filer:	Jonathan R. King/Crystal Corsey
Filer Authorized By:	Jonathan R. King
Attorney Docket Number:	124452.00122
Receipt Date:	03-FEB-2023
Filing Date:	08-AUG-2019
Time Stamp:	13:28:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$170
RAM confirmation Number	E202323D28373658
Deposit Account	022555
Authorized User	Crystal Corsey

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	41200 ddeeed63bd94e617a5747f0f74b6270ce61db976	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38239 4ad9b14d9eef06f7feba662b28c53b90bc3ba2e8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	79439		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO Automated Interview Request (AIR)

Jan 6 2023

This paper requesting to schedule and/or conduct an interview is appropriate because:

This submission is requested to be accepted as an authorization for this interview to communicate via the internet. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned concerning scheduling of the interview via video conference, instant messaging, or electronic mail, and to conduct the interview in accordance with office practice including video conferencing.

Name(s):
Jonathan R King

S-signature:
/Jonathan R King/

Registration Number:
65967

U.S. Application Number:
16535424

Confirmation Number:
2047

E-mail Address:
jrking@blankrome.com

Phone Number:
+1 2155695432

Proposed Time of Interview:
1-17-2023 11:00 AM ET

Alternative Proposed Time(s) of Interview:
1-18-2023 11:00 AM ET

Alternative Proposed Time(s) of Interview:
1-19-2023 11:00 AM ET

Prefered Interview Type:
Telephonic

I am the applicant or applicant's representative for this application.

Topic for Discussion:
Because Applicants representative and Examiners Maccagno and Behncke have conflicting interpretations of the subject matter eligibility guidelines themselves (and not merely on how those guidelines should be applied in this instance), the Applicant respectfully requests that a subject matter eligibility expert from the TQAS attend the agreements. If this request cannot licants representative.

Docket No.: 124452.00122
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert Evan POLLIN et al.

Application No.: 16/535,424 | Confirmation No.: 2047

Filed: August 8, 2019 | Art Unit: 3695

For: ENROLLING A PAYER BY A MERCHANT SERVER OPERATED BY OR FOR THE BENEFIT OF A PAYEE AND PROCESSING A PAYMENT FROM THE PAYER BY A SECURE SERVER | Examiner: Abdulmajeed AZIZ

RESPONSE TO NON-FINAL OFFICE ACTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated October 5, 2022, the Applicant respectfully submits the following:

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 13 of this paper.

The Payment Card Industry (PCI) Data Security Standards (DSS) Requirements and Security Assessment Procedures, Version 2.0 (October 2010) is attached as **Appendix A**.

The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) A-EP and Attestation of Compliance; Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing, Version 3.2.1 (June 2018) is attached as **Appendix B**.

AMENDMENTS TO THE CLAIMS

1. (Currently Amended): A method of processing a payment from a payer to a payee, the method being performed by ~~a secure server~~one or more secure servers, the method comprising:

providing an application programming interface (API) that:

provides an API endpoint that receives ~~receiving~~ an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee;

authenticates the payee;

generates a universal resource locator (URL) for establishing a secure socket layer connection via the internet between the secure server and ~~a computing system used by the payer to receive financial account information provided by the payer~~ the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

establishes the secure socket layer connection between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

outputs instructions to the payer computing system to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide financial account information; and

outputs instructions to the payer computing system to encrypt the financial account information provided by the payer and transmit the encrypted financial account information to the secure server, via the secure socket layer connection, without providing the financial account information to the merchant server;

receiving the financial account information provided by the payer via the secure socket layer connection;

storing the financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

providing an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;

~~storing the financial account information provided by the payer;~~

processing the payment using the financial account information provided by the payer; and

forwarding at least a portion of the payment to the payee.

2. (Previously Presented): The method of claim 1, further comprising:

receiving a second payment transaction instruction from the merchant server, the second payment transaction instruction including a representation of the electronic data token and specifying the amount of the second payment from the payer to the payee;

processing the second payment using the financial account information represented by the electronic data token; and

forwarding at least a portion of the second payment to the payee.

3. (Previously Presented): The method of claim 2, wherein the representation of the electronic data token is the electronic data token.

4. (Currently Amended): The method of claim 1, wherein the payment transaction instruction is generated by the merchant server using ~~an application programming interface~~ the application programming interface provided ~~to the merchant server~~ by the secure server.

5. (Previously Presented): The method of claim 4, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server.

6. (Cancelled)

7. (Previously Presented): The method of claim 4, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

8. - 11. (Cancelled)

12. (Previously Presented): The method of claim 1, wherein the secure connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data provided by the payer.

13. (Original): The method of claim 1, wherein the financial account information includes at least one of a credit card number or bank account number.

14. (Previously Presented): The method of claim 1, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

15. (Previously Presented): The method of claim 1, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

16. (Currently Amended): A secure server that processes a payment from a payer to a payee, the secure server comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the secure ~~computing system~~ server to:

provide an application programming interface (API) configured to:

provide an API endpoint configured to receive an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including at least one data element associated with the payer and specifying an amount of the payment from the payer to the payee;

authenticate the payee;

generate a universal resource locator (URL) to establish a secure socket layer connection via the internet between the secure server and ~~a computing system used by the payer to receive financial account information provided by the payer~~ the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

establish the secure socket layer connection between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

output instructions to the payer computing system to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide financial account information; and

output instructions to the payer computing system to encrypt the financial account information provided by the payer and transmit the encrypted financial account

information to the secure server, via the secure socket layer connection, without providing the financial account information to the merchant server;

receive the financial account information provided by the payer via the secure connection;

store the financial account information in a secure storage location and perform each software process required to maintain compliance with one or more information security standards;

provide an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the data token to the payer;

store the financial account information provided by the payer;

process the payment using the financial account information provided by the payer; and

forward at least a portion of the payment to the payee.

17. (Previously Presented): The secure server of claim 16, wherein the instructions further cause the secure computing system to:

receive a second payment transaction instruction from the merchant server, wherein the second payment transaction instruction includes a representation of the electronic data token and specifies an amount of a second payment from the payer to the payee;

process the second payment using the financial account information represented by the electronic data token; and

forward at least a portion of the second payment to the payee.

18. (Previously Presented): The secure server of claim 17, wherein the representation of the electronic data token is the electronic data token.

19. (Currently Amended): The secure server of claim 16, wherein the payment transaction instruction is generated by the merchant server using ~~an application programming~~

~~interface~~ the application programming interface provided ~~to the merchant server~~ by the secure server.

20. (Previously Presented): The secure server of claim 19, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server.

21. (Cancelled)

22. (Previously Presented): The secure server of claim 19, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

23. - 26. (Cancelled)

27. (Previously Presented): The secure server of claim 16, wherein the secure connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

28. (Previously Presented): The secure server of claim 16, wherein the financial account information includes at least one of a credit card number or bank account number.

29. (Previously Presented): The secure server of claim 16, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

30. (Previously Presented): The secure server of claim 16, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

31. (Previously Presented): A method of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising:

receiving enrollment data identifying a payer;

generating an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a secure connection via the internet between the secure server and a computing system used by the payer for the secure server to receive financial account information provided by the payer;

outputting the electronic instruction to a communications network for transmittal to the secure server;

receiving, from the secure server, an electronic data token representing financial account information received by the secure server via the secure connection, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

storing the electronic data token in association with the enrollment data identifying the payer; and

processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token.

32. (Previously Presented): The method of claim 31, wherein the representation of the electronic data token is the electronic data token.

33. (Previously Presented): The method of claim 31, wherein the electronic instruction is generated using an application programming interface provided to the merchant server by the secure server.

34. (Previously Presented): The method of claim 33, wherein the application programming interface is implemented within a website hosted by the merchant server.

35. (Previously Presented): The method of claim 33, wherein the at least one data element associated with the payer is a customer identifier generated by the merchant server to identify the payer.

36. (Cancelled)

37. (Currently Amended): The method of claim 31, wherein the secure connection is a ~~widget or~~ window or frame within a website provided by the merchant server.

38. (Previously Presented): The method of claim 31, wherein the secure connection provides access to the secure server using a static or dynamic universal resource locator (URL).

39. (Previously Presented): The method of claim 31, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

40. (Previously Presented): The method of claim 31, wherein the secure connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

41. (Previously Presented): The method of claim 31, wherein the enrollment data identifying the payer is received from the payer over a network.

42. (Previously Presented): The method of claim 31, wherein the financial account information includes at least one of a credit card number or bank account number.

43. (Previously Presented): The method of claim 31, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

44. (Previously Presented): The method of claim 31, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

45. (Previously Presented): The method of claim 31, wherein the payment processing system is the secure server.

46. (Previously Presented): A merchant server, operated by or for the benefit of a payee, comprising:

one or more computer processors; and

non-transitory computer readable storage media storing instructions that, when executed by the one or more computer processors, cause the merchant server to:

receive enrollment data identifying a payer;

generate an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a secure connection via the internet between the secure server and a computing system used by the payer for the secure server to receive financial account information provided by the payer;

output the electronic instruction to a communications network for transmittal to the secure server;

receive, from the secure server, an electronic data token representing financial account information received by the secure server provided by the payer via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

store the electronic data token in association with the enrollment data identifying the payer; and

process a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token.

47. (Currently Amended): The merchant server of claim 46, wherein secure connection is a ~~widget or~~ window or frame within a website provided by the merchant server.

48. (New): A method of processing a payment from a payer to a payee, the method being performed by one or more secure servers, the method comprising:

providing an application programming interface (API) that:

provides an API endpoint that receives an electronically-generated payment transaction instruction from a merchant server providing a webpage to a payer computing system used by the payer, the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee;

authenticates the payee;

generates a universal resource locator (URL) for establishing a secure socket layer connection via the internet between the secure server and the payer computing system, the URL comprising either:

a dynamic URL generated by the secure server for the payer and the payee; or

a static URL and a hypertext transport protocol (HTTP) parameter used by the secure server to identify the payer and the payee;

establishes the secure socket layer connection between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;

outputs instructions to the payer computing system to render a financial account registration request form, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide financial account information; and

outputs instructions to the payer computing system to encrypt the financial account information provided by the payer and transmit the encrypted financial account information to the secure server, via the secure socket layer connection, without providing the financial account information to the merchant server;

receiving the financial account information provided by the payer via the secure socket layer connection;

storing the financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

providing an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;

processing the payment using the financial account information provided by the payer; and

forwarding at least a portion of the payment to the payee.

49. (New): The method of claim 48, wherein the URL is a redirect URL that redirects the payer computing system to the secure server.

REMARKS

I. INTRODUCTION

The Office Action dated October 5, 2022 (hereinafter, "the pending Office Action") has been carefully considered. In response thereto, the Applicant respectfully traverses the stated rejection. Accordingly, reconsideration and withdrawal of the outstanding Office Action and issuance of a Notice of Allowance are respectfully solicited in view of the following remarks.

II. STATUS OF THE CLAIMS

Claims 1-7, 9-22, 24-35, and 37-47 are pending. By way of this Amendment, independent claims 1 and 16 are amended to recite features described throughout the specification as originally filed,[1] including providing an application programming interface (API)[2] that authenticates the payee,[3] generates universal resource locator (URL) for establishing a secure socket layer connection between the secure server and the payer computing system (the URL comprising either a dynamic URL[4] generated by the secure server for the payer and the payee or a static URL[5] and a hypertext transport protocol (HTTP) parameter[6] used by the secure server to identify the payer and the payee), establishes the secure socket layer connection within a window or frame that is displayed within a webpage provided by the merchant server,[7] outputs instructions to the payer computing system to render a financial account registration request form (within the window or frame within the webpage provided by the merchant server) that provides functionality for the payer to provide financial account information,[8] and outputs instructions to the payer computing system to encrypt the financial account information provided by the payer and transmit the encrypted financial account information to the secure server (via the secure

[1] The scope of claimed features are not limited by the description in the specification of various exemplary embodiments. However, citations to the specification are provided to show support for newly-claimed features.
[2] *See, e.g.*, paragraphs [0028], [0032], [0056] ("API engine"), FIGS. 4f-4l ("PayAPI"), etc.
[3] *See, e.g.*, FIG. 4f, step 578; paragraph [0072]
[4] *See, e.g.*, FIGS. 4b-4c, paragraph [0059] *et seq.*
[5] *See, e.g.*, FIGS. 4d-4e, paragraph [0066] *et seq.*
[6] For example, the "session identifier" of paragraph [0072], etc.
[7] *See, e.g.*, paragraphs [0059], [0067], etc.
[8] *See, e.g.*, paragraphs [0060], [0067]-[0068], etc.

socket layer connection) without providing the financial account information to the merchant server.[9]

Independent claims 1 and 16 are also amended to further recite storing the financial account information in a secure storage location[10] and performing each software process required to maintain compliance[11] with one or more information security standards.[12]

Dependent claims 6 and 21 are amended for consistency with independent claims 1 and 15 and dependent claims 9-11 and 24-26 are cancelled. New independent claim 48 is added, which recites many of the features of independent claim 16. New dependent claim 49 is added to recite the features previously recited in newly-cancelled dependent claim 26.

No new matter is added.

III. SUMMARY OF THE OFFICE ACTION

In the pending Office Action, the pending claims are rejected under 35 U.S.C. § 101 as allegedly directed to non-patent eligible subject matter.

IV. PATENT ELIGIBLE SUBJECT MATTER REJECTION (35 U.S.C. § 101)

As described in the previously-filed Amendment, shown in the attached documentary evidence, and discussed below, electronic payment processing is a technical process (Section A) and the claimed invention improves both the prior art technology itself and the prior art technical process by eliminating the need for prior art merchant servers to include numerous components and to perform numerous computer processing steps (Section E), eliminating redundant computer components and redundant processing steps (Section F), eliminating the need to ensure that payment processing components and processes do not negatively impact merchant

[9] *See, e.g.*, paragraphs [0062]-[0063], [0069]-[0070], etc.
[10] *See, e.g.*, paragraphs [0011], [0056], etc.
[11] *See, e.g.*, paragraph [0005] ("Underlying software applications may require substantial modifications to achieve compliance"; "security … measures required to comply") and [0052] ("The secure server 202 or "hosted system" preferably meets acknowledged security standards, such as the PCI standard, to safeguard the financial account information secured there.")
[12] For example, the Payment Card Industry (PCI) Data Security Standard (DSS) information security standard described in paragraphs [0004]-[0005].

functionality or customer experience (Section G), and eliminate the need for merchant organizations to perform numerous tasks (Section H).

The pending Office Action repeats those specific factual assertions but does not actually address them. Instead, the pending Office Action asserts that the specification does not describe a technological problem,[13] argues that electronic payment processing in general (and all but eight words of independent claim 1 in particular) is "a method of organizing human activity,"[14] asserts – without evidence – that the claimed ordered combination of processing steps is "conventional",[15] and concludes – again, without addressing any of the specific factual assertions or documentary evidence to the contrary – that "there are no improvements to another technology or technical field [and] no improvements to the functioning of the computer itself".[16]

The Applicant respectfully traverses the stated rejection. As described in detail below, electronic payment processing is a technical process (Section A), the claimed ordered combination of specific processing steps are "additional elements" (Section B) that are not "conventional" (Section C), the specification identifies a technical problem and describes a technical solution (Section D), and the claimed invention improves both the prior art technology itself and the prior art technical process by eliminating the need for prior art merchant servers to include numerous components and to perform numerous computer processing steps (Section E), eliminating redundant computer components and redundant processing steps (Section F), eliminating the need to ensure that payment processing components and processes do not negatively impact merchant functionality or customer experience (Section G), and eliminate the need for merchant organizations to perform numerous tasks (Section H).

A. Electronic payment processing is not "a method of organizing human activity"

The Federal Circuit has held that inventions engineered in the context of serving potential customers and merchants are patent eligible if "the invention [is] not claiming a business method

[13] Pages 13-14
[14] Pages 27-28
[15] Pages 7-8
[16] Page 7

per se, but [is] instead claiming a technical way to satisfy an existing problem for website hosts and viewers."[17] Similarly, while the invention at issue is used in service of a business transaction, the claims are not directed to a process for marketing or arranging that business transaction, but are instead directed to a system for electronically processing a payment via the internet.

To that end, independent claims 1 and 16 recite a secure server and application programming interface (API) that receive an electronically-generated payment transaction instruction from a merchant server (providing a webpage to a payer computing system), authenticate the merchant, generate a URL for establishing a secure socket layer connection between the secure server and the payer computing system, output instructions to the payer computing system to render a financial account registration request form (that provides functionality for the payer to provide financial account information) within a window or frame that is displayed within the webpage provided by the merchant server, output instructions to the payer computing system to encrypt the financial account information and transmit the encrypted financial account information via the secure socket layer connection, receive the financial account information via the secure socket layer connection, provide an electronic data token (representing the financial account information provided by the payer) to the merchant server, and process the payment using the financial account information.

Furthermore, independent claims 1 and 16 recite that the secure server stores the financial account information in a secure storage location and performs each software process required to maintain compliance with one or more information security standards. Meanwhile, as shown in the attached Exhibit A and enumerated in Section E below, in some instances the hardware components required for "secure storage" and the software processes "required to maintain compliance" include rendering any primary account number (PAN) unreadable anywhere it is stored (by one-way hashing the entire PAN using strong cryptography, using index tokens and securely stored pads, or using strong cryptography with associated key-management processes and procedures, masking PAN when displayed, generating strong data-encrypting cryptographic

[17] *BASCOM v. AT&T Mobility*, 827 F.3d 1341, 1351 (Fed. Cir. 2016) characterizing the claims at issue in *DDR Holdings, v. Hotels.com*, 773 F.3d 1245 (Fed. Cir. 2016)

keys, encrypting those data-encrypting cryptographic keys using key-encrypting cryptographic keys, storing the key-encrypting cryptographic keys separately from the data-encrypting cryptographic keys, securely distribute the data-encrypting cryptographic keys, changing cryptographic keys that reach the end of their cryptoperiod, functionality to retire or replace cryptographic keys when required (for example, by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys, e.g., using a key encryption key), managing logical access to disk encryption independently of native operating system access control mechanisms, functionality to manage manual clear-text cryptographic key management operations using split knowledge and dual control, a programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy, a process to securely delete sensitive authentication data received from cardholders, strong cryptography and security protocols (e.g., SSL/TLS, IPSEC, or SSH) to safeguard sensitive cardholder data transmitted over open, public networks, systems configured to accept only trusted cryptographic keys and/or certificates, a protocol implemented to use only secure configurations (that did not support insecure versions or configurations), use of "the proper encryption strength" (according to vendor recommendations/best practices) for the encryption methodology in use, rendering PAN unreadable or secured with strong cryptography when sent to end-user messaging technologies, wireless networks that use industry best practices to implement strong encryption for authentication or transmission (e.g., Advanced Encryption Standard block cipher, which requires a dedicated chip that was not commonly included in most wireless network hardware).

None of those software processes (or hardware components) recited in the claims or required to maintain compliance organize human activity. The pending Office Action argues that the claims are directed to a "fundamental economic practice or commercial or legal interaction".[18] However, unlike the patent-ineligible claims described in MPEP §2106.04(a)(2)(II), the claims at issue are not directed to an economic practice itself (such as

[18] Page 28

offer-based price optimization[19] or financial instruments designed to protect against the risk[20]), an "agreement in the form of contacts" (such as managing a stable value protected life insurance policy[21] or processing insurance claims for a covered loss or policy event under an insurance policy[22]), a "legal obligation" (such as hedging,[23] mitigating settlement risk,[24] or arbitration[25]) or "advertising, marketing or sales activities or behaviors" (such as structuring a sales force or marketing company,[26] or determining the optimal number of visits by a business representative[27]). In other words, the claims are not directed to a commercial interaction itself, but rather to a specific technical process for electronically processing a payment in connection with that commercial interaction.

B. The specific processing steps recited in the claims are "more than simply stating the [concept of processing a payment from a payee to a payer] while adding the words 'apply it'" (or an equivalent)[28]

The stated rejection is that, except for eight words (server, electronic, secure connection, computing system, and communications network), all of the features recited the claims are directed to the abstract idea of "processing a payment from a payer to a payee." Meanwhile, the pending Office Action asserts[29] that the ordered combination of specific processing steps recited in the claims amounts to "merely reciting the words 'apply it' (or an equivalent) with the judicial exception".[30]

Even if the Patent Office asserts that the broad concept of "processing a payment from a payer to a payee" is a judicial exception under § 101, the ordered combination of specific processing steps recited in the claims – rather than eight individual words – are "additional

---

[19] *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63, 115 USPQ2d 1090, 1092-93 (Fed. Cir. 2015)
[20] *In re Chorna*, 656 Fed. App'x 1016, 1021 (Fed. Cir. 2016) (non-precedential)
[21] *Bancorp Servs., LLC v. Sun Life Assur. Co. of Canada (U.S.)*, 687 F.3d 1266, 1280 (Fed. Cir. 2012)
[22] *Accenture Global Services v. Guidewire Software, Inc.*, 728 F.3d 1336, 1338-39 (Fed. Cir. 2013)
[23] *Bilski v. Kappos*, 561 U.S. 593, 595 (2010);
[24] *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 218 (2014)
[25] *In re Comiskey*, 554 F.3d 967, 981 (Fed. Cir. 2009).
[26] *In re Ferguson*, 558 F.3d 1359, 1364 (Fed. Cir. 2009)
[27] *In re Maucorps*, 609 F.2d 481, 485, 203 USPQ 812, 816 (CCPA 1979);
[28] MPEP § 2106.05(f)
[29] Pages 7, 9, and 21, referring to "the 'apply-it' standard"
[30] MPEP § 2106.04(d)(I)

elements." After all, the ordered combination of specific processing steps recited in the claims is not a "building blocks of human ingenuity" or one of "the basic tools of scientific and technological work." Meanwhile, those specific processing steps cannot be characterized as "a drafting effort designed to monopolize" the broad concept of "processing a payment from a payer to a payee." Rather, systems can – and often do – process payments without the use of a secure server performing the specific processing steps recited in the claims.

Nevertheless, in an effort to advance prosecution, independent claims 1 and 16 are amended to further recite additional technical processing steps that enable the claimed secure server to solve the technical problems and provide the technical benefits outlined below. Claim 1 recites (emphasis added):

> 1. A method of processing a payment from a payer to a payee, the method being performed by **one or more secure servers**, the method comprising:
>
> **providing an application programming interface (API)** that:
>
> provides **an API endpoint that receives an electronically-generated payment transaction instruction** from a merchant server providing a webpage to a payer computing device used by the payer, the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee;
>
> **authenticates the payee;**
>
> **generates universal resource locator (URL) for establishing a secure socket layer connection via the internet between the secure server and the payer computing system**, the URL comprising either:
>
> **a dynamic URL** generated by the secure server for the payer and the payee; or
>
> **a static URL and a hypertext transport protocol (HTTP) parameter** used by the secure server to identify the payer and the payee;
>
> **establishes the secure socket layer connection between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server;**
>
> outputs **instructions to the payer computing system to render a financial account registration request form**, within the window or frame that is displayed within the webpage provided by the merchant server, that provides functionality for the payer to provide financial account information; and
>
> outputs **instructions to the payer computing system to encrypt the financial account information** provided by the payer **and transmit the encrypted financial account information** to the secure server, **via the secure socket layer connection**, without providing the financial account information to the merchant server;

receiving the financial account information provided by the payer via the secure socket layer connection;

storing the financial account information in a secure storage location and performing each software process required to maintain compliance with one or more information security standards;

providing an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;

processing the payment using the financial account information provided by the payer; and

forwarding at least a portion of the payment to the payee.

The Applicant respectfully submits that, particularly as an ordered combination, the specific processing steps shown above (e.g., in bold) were not "well-understood, routine or conventional", would not "monopolize" the broad concept of "processing a payment from a payer to a payee" through the grant of a patent, and integrate that broad concept into a practical application for at least the reasons described below.

C. Whether the processing steps recited in the claims were "conventional" should not be considered in Step 2A Prong Two and, in Step 2B, requires factual evidence that the ordered combination of processing steps was so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement of 35 U.S.C. § 112(a)

The pending Office Action repeatedly argues that a judicial exception has not been integrated into a practical application under Step 2A Prong Two because processing steps recited in the claims are "conventional".[31] However, the subject matter eligibility guidelines specifically state that examiners should "give weight to all additional elements" in Step 2A regardless of "whether or not they are conventional".[32]

[31] Pages 8 and 14

[32] "Step 2A specifically excludes consideration of whether the additional elements represent well-understood, routine, conventional activity. Accordingly, in Step 2A Prong Two, examiners should ensure that they give weight to all additional elements, whether or not they are conventional, when evaluating whether a judicial exception has been integrated into a practical application. Additional elements that represent well-understood, routine, conventional activity may integrate a recited judicial exception into a practical application." MPEP § 2106.04(d)(I)

Meanwhile, in Step 2B, "a factual determination is required to support a conclusion that an additional element (or combination of additional elements) is well-understood, routine, conventional activity."[33] To support such a conclusion, the subject matter eligibility guidelines require factual evidence that the specific "combination"[34] of elements recited in the claims were so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement of 35 U.S.C. § 112(a).[35]

The pending Office Action argues that the Examiner did not apply the "well-known and conventional WURC standard":

> Per the 101 rejection below, the claims do not recite significantly more. It's not clear how the solution overcomes the "apply-it" standard regarded in the rejection (applicant points to the well-known and conventional WURC standard, which the Examiner did not apply in the rejection).[36]

However, the subject matter eligibility guidelines state that "when making a determination whether the additional elements in a claim amount to significantly more than a judicial exception, the examiner should evaluate whether the elements define only well-understood, routine, conventional activity."[37] In this instance, the pending Office Action provides no evidence that the ordered combination of specific processing steps recited in the claims was "conventional" as asserted in the pending Office Action, let alone so "widely prevalent" that they did not need description in a patent specification.

D. The specification identifies a technical problem and identifies technical improvements realized by the claims over the prior art

The pending Office Action argues that the "specification in the instant application does not … describe technological problems with a technological solution" and instead "describes a

[33] MPEP § 2106.05(d)(I)(2) citing *Berkheimer v. HP, Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018)
[34] MPEP § 2106.05(e) citing *BASCOM*, 827 F.3d at 1349
[35] MPEP § 2106.05(d)(I)(1)
[36] Pages 8 and 14
[37] MPEP § 2106.05(d)(I)

recognized business problem with a solution in the computer arts where a server is used to process information and perform computationally-intensive analysis for other locations."[38]

As an initial matter, there is no requirement under § 101 that the claims address a technical problem[39] or that the technological problem be described in the specification.[40] Additionally, the problem described in the specification is that maintaining compliance with an information security standard like the PCI Data Security Standard requires both organizational measures and "software applications" that perform "security ... measures required to comply with the PCI standards" and "may require substantial modifications to achieve compliance":

> [0003] Fraud in credit card and other financial transactions is a major problem, and **considerable resources are devoted to securing credit card and other account information provided to merchants by payers**. ...
>
> [0004] The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
>
> [0005] Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud. ... **The security** and organizational **measures required to comply with the PCI standards**, and the cost of the annual audits, **are borne by the individual organization. Underlying software applications may require substantial modifications to achieve compliance**, and significant changes in organizational structure and operating procedures may also be required. **Thus, the time, effort, and cost required for merchants and processors to obtain PCI certification to receive and use credit card data are substantial.**

The specification then goes on to describe an unconventional technical solution, recited in the pending claims, that overcomes that technical problem (by eliminating the need for a merchant server 204 to include the components and perform the software processing steps

---

[38] Page 14

[39] For instance, in *DDR Holdings, v. Hotels.com*, 773 F.3d 1245, 1257, the problem addressed by the claimed invention was that "upon the click of an advertisement for a third-party product displayed on a host's website," the host website would lose that visitor as he or she is "transported to the third party's website."

[40] "The specification need not explicitly set forth" an improvement to the functioning of a computer or another technology or technical field, but rather "it must describe the invention such that the improvement would be apparent to one of ordinary skill in the art." MPEP § 2106.04(d)(1). Here, those of ordinary skill in the art would have been aware of the technical challenges of complying with data security standards (such as the PCI standard attached as Appendix A) referenced in the specification.

required to maintain compliance), thereby reducing the time and cost of developing the merchant server 204:

> [0028] … Using the methods disclosed herein, in preferred embodiments merchants are able to process such transactions without transmitting, processing or storing Financial Account data. This reduces the potential liability of the merchants for data loss, and avoids placing their customer tracking and payment processing systems (such as merchant server 204) within the scope of the present Payment Card Industry Data Security Standard (PCI-DSS), thus **reducing compliance costs, development costs, and accelerating time-to-market.**

The pending Office Action argues that "the specification describes a recognized business problem".[41] However, the Applicant respectfully submits that the fact that "underlying software applications may require substantial modifications" in order to perform the "security … measures required to comply" with an information security standard is a technical problem, as is the desire to reduce "development costs" and "accelerat[e] time-to-market."

E. The claimed invention improves the functioning of the prior art merchant server itself by eliminating the need for the merchant server to "store financial account information in a secure storage location and perform each software process required to maintain compliance with one or more information security standards"

By eliminating the need for merchant servers to receive, store, and transmit financial account information, the claimed invention eliminates the need for those merchant servers to include the hardware components and perform the software processes required to maintain compliance with information security standards, like the PCI Data Security Standard that was in place on the effective filing date of the present application[42] that is attached as Appendix A. Instead, in the years since the claimed invention has become available, the Payment Card Industry Security Standards Council has published requirements,[43] attached as Appendix B, that are applicable to e-commerce merchants with websites that do not receive cardholder data and

---

[41] Page 14
[42] PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (October 2010) (hereinafter, "PCI DSS v2.0")
[43] PCI Data Security Standard Self-Assessment Questionnaire (SAQ) A-EP and Attestation of Compliance; Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing, Version 3.2.1 (June 2018) (hereinafter, "PCI DSS v3.2.1 SAQ A-EP")

outsource their e-commerce payment channel to a PCI DSS validated third-party payment processor.[44]

To comply with the information security standard of Appendix A prior to the claimed invention, prior art merchant systems were required to protect stored cardholder data by rendering any primary account number (PAN) unreadable anywhere it is stored[45] by one-way hashing the entire PAN using strong cryptography, using index tokens and securely stored pads, or using strong cryptography with associated key-management processes and procedures.[46]

Prior art merchant systems were required to generate strong data-encrypting cryptographic keys,[47] encrypt those data-encrypting cryptographic keys using key-encrypting cryptographic keys,[48] store the key-encrypting cryptographic keys separately from the data-encrypting cryptographic keys,[49] and securely distribute the data-encrypting cryptographic keys.[50] Prior art merchant systems were required to change cryptographic keys that had reached the end of their cryptoperiod (e.g., after a defined period of time and/or a defined amount of ciphertext had been produced).[51] Prior art merchant systems were also required to include functionality to retire or replace cryptographic keys when required,[52] for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key).[53] Prior art merchant systems were also required to mask PAN when displayed.[54]

---

[44] Page iii
[45] including on portable digital media, backup media, and in logs
[46] Requirement 3.4. If the "full PAN is not needed" (page 28), the PCI Data Security Standard also permitted truncation of cardholder data as long as truncated segment of the PAN was not hashed. However, to process a payment, prior art merchant systems needed to store the full PAN.
[47] Requirement 3.6.1
[48] Requirements 3.5.2, Testing Procedure 3.5.2.a
[49] *Ibid.*
[50] Requirement 3.6.2
[51] Requirement 3.6.4
[52] The retirement or replacement of a cryptographic key was required if the cryptographic key was suspected of being compromised or when the integrity of the cryptographic key had been weakened (for example, if an employee with knowledge of a clear-text cryptographic key left the organization)
[53] Requirement 3.6.5
[54] Requirement 3.3

If the prior art merchant system used disk encryption,[55] the prior art merchant system was required to manage logical access independently of native operating system access control mechanisms.[56] A prior art merchant system was not compliant with the PCI Data Security Standard if it used local user account databases or tied decryption keys to user accounts.[57]

If the prior art merchant system used manual clear-text cryptographic key management operations, the prior art merchant system was required to provide functionality to manage those operations using split knowledge and dual control.[58] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key.[59]

To avoid the requirement to conduct quarterly manual reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy, a prior art merchant system was required to include a programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy.[60]

Except in limited circumstances,[61] prior art merchant systems were required to perform a process to securely delete sensitive authentication data received from cardholders, including the full contents of any magnetic stripe or chip,[62] any card validation code,[63] and any personal identification number (PIN) or encrypted PIN block.[64] While merchant systems that partially outsource their e-commerce payment channel using the claimed invention are still required to securely delete any sensitive authentication data they receive,[65] the claimed invention allows merchant systems to process payments without receiving any sensitive authentication data.

---

[55] rather than file- or column-level database encryption
[56] Requirement 3.4.1
[57] *Ibid.*
[58] Requirement 3.6.6
[59] *Ibid.*
[60] Requirement 3.1.1, Testing Procedure 3.1.1.d
[61] Issuers and companies that support issuing services were permitted to securely store sensitive authentication data if there was "a business justification" to store that sensitive authentication data
[62] Requirement 3.2.1
[63] Requirement 3.2.2
[64] Requirement 3.2.3
[65] PCI DSS v3.2.1 SAQ A-EP, Requirement 3

Prior art merchant systems were required to use strong cryptography and security protocols to safeguard sensitive cardholder data transmitted over open, public networks such as the Internet, wireless networks, and mobile networks.[66] The PCI Data Security Standard suggested using SSL/TLS, IPSEC, or SSH to transmit sensitive cardholder data over open, public networks.[67] Prior art merchant systems were required to accept only trusted cryptographic keys and/or certificates,[68] to use a protocol implemented to use only secure configurations (that did not support insecure versions or configurations),[69] and to use "the proper encryption strength" (according to vendor recommendations/best practices) for the encryption methodology in use.[70] Prior art merchant systems were required to render PAN unreadable or secured with strong cryptography whenever sent to end-user messaging technologies such as email, instant messaging, or chat programs.[71] Again, merchants who partially outsource their e-commerce payment channel using the claimed invention are still required to safeguard any sensitive cardholder data they transmit.[72] However, the claimed invention allows merchant systems to process payments without transmitting any sensitive cardholder data.

Wireless networks transmitting cardholder data or connected to the cardholder data environment were required to use industry best practices to implement strong encryption for authentication or transmission.[73] The PCI Data Security Standard noted that the use of Wired Equivalent Privacy (WEP) as a security control was prohibited and suggested IEEE 802.11i as an example of industry best practices.[74] Note that the IEEE 802.11i standard makes use of the Advanced Encryption Standard (AES) block cipher, which requires a dedicated chip that was not commonly included in most wireless network hardware.[75]

---

[66] PCI DSS v2.0, Requirement 4.1
[67] *Ibid.*
[68] Requirement 4.1, Testing Procedure 4.1.b
[69] Requirement 4.1, Testing Procedure 4.1.c
[70] Requirement 4.1, Testing Procedure 4.1.d
[71] Requirement 4.2, Testing Procedure 4.2.a
[72] PCI DSS v3.2.1 SAQ A-EP, Requirement 4
[73] PCI DSS v2.0, Requirement 4.1.1
[74] *Ibid.*
[75] See 802.11i, TechTarget, June 2006, https://www.techtarget.com/searchmobilecomputing/definition/80211i

The pending Office Action argues that "outsourcing the processing to another device does not meaningfully reduce the processing that needs to occur in maintaining PCI compliance."[76] However, as described above, the claimed invention reduces the processing that needs to be performed by the merchant server (and components that need to be included in the merchant system), thereby improving the functioning of the merchant server. Meanwhile, as described below in Section F, outsourcing payment processing to a secure server that provides functionality for multiple merchant servers significantly reduces the processing that needs to occur.

F. Additionally, because the secure server recited in the claims can process payments for multiple merchant servers, the claimed invention improves the functioning of the combined system (i.e., both the merchant servers and the secure server) by eliminating redundant computer components and redundant processing steps

The claimed invention allows multiple merchant systems to outsource the processing of cardholder data to the secure server recited in the claims while maintaining PCI compliance as described in the PCI Data Security Standard of Appendix B. Accordingly, rather than *each* merchant system being required to include the required computer components, only the secure server is required to include many of the computer components required by the PCI Data Security Standard of Appendix A. Additionally, rather than *each* merchant system being required to perform each of the software processing steps required by the PCI Data Security Standard of Appendix A, many of those software processing steps are only required to be performed once by the secure server recited in the claims for each of those merchant systems to maintain PCI compliance.

By providing a financial account registration request form to payers of multiple merchants via an application programming interface (for example, within windows or frames that are displayed within the webpages provided by those merchant servers), the secure server can provide a single interface that masks that PAN when displayed,[77] a single process to remove

[76] Page 9
[77] PCI DSS v2.0, Requirement 3.3

stored cardholder data exceeding the requirements defined in the secure system's data retention policy,[78] and a single process to securely delete sensitive authentication data.[79]

The secure system can protect that cardholder data for all of those merchant systems by generating strong data-encrypting cryptographic keys, encrypting those data-encrypting cryptographic keys using key-encrypting cryptographic keys, securely storing the cryptographic keys, and retiring or replacing the cryptographic keys when required.[80] One particularly beneficial improvement provided by the claimed invention is the secure system can perform a single key rotation process and ensure that all cryptographic keys used for all merchants are changed before they reach the end of their cryptoperiod.[81]

While receiving and transmitting sensitive cardholder data for multiple merchants, the secure server recited in the claims only requires one set of components that uses strong cryptography and security protocols to safeguard that sensitive cardholder data during transmission over open, public networks[82] (including wireless network hardware with the dedicated chip[83] required by the IEEE 802.11i standard[84] if needed to transmit cardholder data wirelessly).

Again, the pending Office Action argues that "outsourcing the processing to another device does not meaningfully reduce the processing that needs to occur in maintaining PCI compliance." However, as described above, outsourcing payment processing to a secure server that provides functionality for multiple merchant servers significantly reduces the components needed for compliance and the processing that needs to occur.

---

[78] Requirement 3.1.1, Testing Procedure 3.1.1.d
[79] Requirement 3.2
[80] Requirement 3.4 through Requirement 3.6
[81] Requirement 3.6.4
[82] Requirement 4.1
[83] *See* 802.11i, TechTarget, June 2006, https://www.techtarget.com/searchmobilecomputing/definition/80211i
[84] PCI DSS v2.0, Requirement 4.1.1

G. The claimed invention improves the prior art electronic payment processing processes by eliminating the need for merchants to ensure that the components and processes required to maintain compliance with an information security standard do not negatively impact the merchant functionality and customer experience

Prior to the claimed invention, merchants were required to integrate their systems with the computer components required for compliance described above while ensuring that those components did not negatively impact the functions performed by the merchant system, including the user experience provided to their customers. By enabling those merchants to outsource the processing of cardholder data to the secure server recited in the claims and simply request, via an API, that the claimed secure server provide a financial account registration request form (in a window or frame within the webpage provided by the merchant server[85] or a separate webpage[86]), the secure server and merchant server recited in the claims form a hybrid system (similar to the hybrid webpage[87] at issue in *DDR*[88]) that enables merchants to focus their efforts on their own core systems – and the user experience provided to their customers – while maintaining compliance with an information security standard.

The pending Office Action argues that "it's not clear how" the claimed processing steps "impose[] a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception." First, as described above, those specific processing steps are hardly "a drafting effort designed to monopolize the judicial exception" of "processing a payment from a payer to a payee", as systems can – and do – process payments from a payer to a payee without the use of a separate secure server, let alone one that provides an API, authenticates the payee, generates universal resource locator (URL) for

[85] as recited in independent claims 1 and 16
[86] see, e.g., dependent claim 49
[87] Note that, in the embodiments of claims 1 and 16, the "secure socket layer connection between the secure server and the payer computing system within a window or frame that is displayed within the webpage provided by the merchant server" is strikingly similar to the solution in *DDR* in that it is "an automatically-generated hybrid web page that combines visual 'look and feel' elements" from the merchant server website and functionality to provide financial account information to the third-party secure server. In those embodiments, the merchant server sends its visitors to a website "that 1) incorporates 'look and feel' elements from the [merchant server] website, and 2) provides visitors with the opportunity" to submit sensitive financial account information to the third-party secure server "without actually entering" that secure server's website.
[88] *DDR*, 773 F.3d at 1257-58

establishing a secure socket layer connection, etc. Additionally, the claimed invention "integrates the judicial exception" by improving the prior art electronic payment processing process. In this section in particular, the Applicant points out that the claimed system eliminates the need for merchants to ensure that the components and processes required to maintain compliance with an information security standard do not negatively impact the merchant functionality and customer experience. Instead, those merchants can focus their efforts on their own merchant functionality– and the user experience provided to their customers – and simply request, via an API, that the claimed secure server provide the claimed financial account registration request form (e.g., in a window or frame within the webpage provided by the merchant server[89]).

The pending Office Action also argues that the claims are distinguishable from *DDR* because "the claimed solution is not necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer [networks]".[90] However, the Applicant respectfully submits that *the need to securely receive and store sensitive data while electronically processing payments to comply with information security standards required for electronic payment processors* is a problem "specifically arising in the realm of computer networks", as is the specific problem described above of *ensuring that those components and processes do not negatively impact the merchant functionality and customer experience at an online retailer*. Moreover, the claimed secure server performing the claimed processing steps is a solution "rooted in computer technology".

H. Additionally, the claimed invention improves prior art electronic payment processing methods by eliminating the need for each merchant to perform numerous organizational tasks to comply with an information security standard

Another way that patent eligible inventions can improve a technological process is by reducing the time necessary for humans to maintain that technology. For example, the Federal Circuit in *BASCOM* held that filtering content at the ISP server (rather than on each end-user's

[89] as recited in independent claims 1 and 16
[90] Page 15

client machine) was patent eligible under § 101 because it eliminated the "difficult and time consuming" process of installing software "on every end-user's client machine."[91]

In addition to the required computer components and computer processing steps outlined above, the PCI Data Security Standard also required that employees or agents of merchants using prior art merchant systems perform all of the organizational tasks outlined in detail below.

As an initial matter, merchants using prior art merchant systems were required to verify that the prior art merchant systems complied with each and every one of the requirements above. Additionally, protect stored cardholder data, merchants were required to implement data retention and disposal policies, procedures, and processes to keep cardholder data storage to a minimum.[92] To comply with the PCI Data Security Standard, the data retention and disposal policy was required to limit data storage and retention time "to that which is required for legal, regulatory, and business requirements."[93] Merchants were required to have specific retention requirements for all cardholder data[94] specifying the time period that cardholder data needed to be stored and the legal, regulatory, or business reason why that cardholder data needed to be stored for that time period.[95] The data retention and disposal policy was also required to include provisions for secure disposal of data (including disposal of cardholder data) when no longer needed for those legal, regulatory, or business reasons.[96] If the merchant system did not include the programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy, the merchant was required to conduct quarterly reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy.[97]

Merchants were required to examine data sources – including incoming transaction data, all logs (e.g., transaction logs, history logs, debugging logs, and error logs), history files, trace

---

[91] *BASCOM*, 827 F.3d at 1344
[92] Requirement 3.1
[93] Requirement 3.1.1
[94] Requirement 3.1.1, Testing Procedure 3.1.1.c
[95] Requirement 3.1.1, Testing Procedure 3.1.1.a
[96] Requirement 3.1.1, Testing Procedure 3.1.1.b
[97] Requirement 3.1.1, Testing Procedure 3.1.1.d

files, several database schemas, and database contents – to verify that the full contents of magnetic stripes or chips,[98] card validation codes,[99] and PINs or encrypted PIN blocks[100] were not stored under any circumstance.

To verify that displayed PAN was masked, merchants were required to obtain and examine writing policies and examine displays of PAN (e.g., on screen or on paper receipts) to verify that the PAN was masked[101] and examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[102]

To verify that stored PAN was rendered unreadable, merchants were required to examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[103] Additionally, merchants were required to confirm that PAN was rendered unreadable by examining several tables or files from a sample of data repositories,[104] a sample of removable media (e.g., back-up tapes),[105] and a sample of audit logs.[106]

To protect cryptographic keys, merchants were required to document and implement key-management processes and procedures.[107] The key-management processes and procedures were required to restrict access to the fewest number of custodians necessary[108] and to store cryptographic keys in the fewest possible locations and forms.[109] Merchants were required to periodically change cryptographic keys once they reached the end of their cryptoperiod (for example, as after a defined period of time had passed and/or after a defined amount of cipher-text had been produced) as defined by the associated application vendor or key owner and based

[98] Requirement, 3.2.1, Testing Procedure 3.2.1
[99] Requirement, 3.2.2, Testing Procedure 3.2.2
[100] Requirement, 3.2.3, Testing Procedure 3.2.3
[101] Requirement 3.3, Testing Procedure 3.3
[102] Requirement, 3.4, Testing Procedure 3.4.a
[103] Requirement, 3.4, Testing Procedure 3.4.a
[104] Requirement, 3.4, Testing Procedure 3.4.a
[105] Requirement, 3.4, Testing Procedure 3.4.c
[106] Requirement, 3.4, Testing Procedure 3.4.d
[107] Requirement 3.6
[108] Requirement 3.5.1
[109] Requirement 3.5.2, Testing Procedure 3.5.2.b

on industry best practices and guidelines (e.g., NIST Special Publication 800-57).[110] Merchants were also required to retire or replace cryptographic keys if the cryptographic key was suspected of being compromised[111] or when the integrity of the cryptographic key had been weakened (for example, if an employee with knowledge of a clear-text cryptographic key left the organization),[112] for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key).[113]

If the merchant system used manual clear-text cryptographic key management operations, the merchant was required to manage those operations using split knowledge and dual control.[114] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key.[115] The merchant key-management procedures were required to prevent unauthorize substitution of cryptographic keys.[116] Merchants were required to obtain written or electronic acknowledgement from all custodians of the cryptographic keys that those custodians understood and accepted their key-custodian responsibilities.[117]

Merchants were required to observe a sample of transactions as they occurred to verify that cardholder data was encrypted during transit.[118] For SSL/TLS implementations, merchants were required to verify that HTTPS appeared as a part of the browser Universal Record Locator (URL) and that no cardholder data was required when HTTPS does not appear in the URL.[119] Merchants were also required to maintain a policy stating that unprotected PANs were not to be sent via end-user messaging technologies.[120]

---

[110] Requirement 3.6.4
[111] Requirement 3.6.5, Testing Procedure 3.6.5.b
[112] Requirement 3.6.5, Testing Procedure 3.6.5.a
[113] Requirement 3.6.5
[114] Requirement 3.6.6
[115] *Ibid.*
[116] Requirement 3.5.7, Testing Procedure 3.6.7
[117] Requirement 3.5.8, Testing Procedure 3.6.8
[118] Requirement 4.1, Testing Procedure 4.1.a
[119] Requirement 4.1, Testing Procedure 4.1.e
[120] Requirement 4.2, Testing Procedure 4.2.b

By providing functionality for multiple merchants to outsource the processing of cardholder data, the claimed invention improves the prior art process of processing a payment by eliminating the need for each merchant to individually perform each of the organizational tasks above.

The pending Office Action asks "How is this invention like Bascom?"[121] In both instances, one prior art solution was to install separate software on multiple, separate computing devices (separate internet content filters "on every end-user's client machine" and separate information security standard-compliant payment processing devices for each of a number of merchants). One problem addressed by the claimed invention in *BASCOM* was that it was "difficult and time consuming" to install the software and update the client database on every end-user's client machine. Similarly, to maintain compliance as described above, each merchant must each perform all of the required organizational tasks. The claimed solution in *BASCOM* was to instead use a remote server at the ISP to perform internet content filtering for each end-user client machine, eliminating the time and difficulty of providing and maintaining separate software instances for each of a number of end users. Similarly, by providing functionality for multiple merchants to outsource the processing of cardholder data, the claimed invention eliminates the need for each merchant to individually perform each of the organizational tasks identified above.

Accordingly, the Applicant respectfully submits that the pending claims are patent eligible subject matter under § 101.

V. CONCLUSION

In view of the above Remarks, the Applicant believes the pending application is in condition for allowance.

Please charge any shortage or credit any overpayment of fees to BLANK ROME LLP, Deposit Account No. 23-2185, under Order No. 124452.00122. In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition

[121] Page 14

does not accompany this Amendment or is insufficient to render this Amendment timely, the Applicant hereby petitions under 37 C.F.R. §1.136(a) for an extension of time for as many months as required to render this submission timely. Any fee due is authorized above.

Dated: January 5, 2023

Respectfully submitted,

By: /Michael C. Greenbaum/
Michael C. Greenbaum
Registration No.: 28,419
BLANK ROME LLP
Correspondence Customer Number: 27557
Attorney for Applicant

Appendix A



Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

Document Changes

Date	Version	Description	Pages
October 2008	*1.2*	*To introduce PCI DSS v1.2 as "PCI DSS Requirements and Security Assessment Procedures," eliminating redundancy between documents, and make both general and specific changes from* PCI DSS Security Audit Procedures v1.1. *For complete information, see* PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2.	
July 2009	*1.2.1*	*Add sentence that was incorrectly deleted between PCI DSS v1.1 and v1.2.*	*5*
		Correct "then" to "than" in testing procedures 6.3.7.a and 6.3.7.b.	*32*
		Remove grayed-out marking for "in place" and "not in place" columns in testing procedure 6.5.b.	*33*
		For Compensating Controls Worksheet – Completed Example, correct wording at top of page to say "Use this worksheet to define compensating controls for any requirement noted as 'in place' via compensating controls."	*64*
October 2010	*2.0*	*Update and implement changes from v1.2.1. For details, please see "*PCI DSS - Summary of Changes from PCI DSS Version 1.2.1 to 2.0."	

Copyright 2010 PCI Security Standards Council LLC



Table of Contents

Document Changes 2
Introduction and PCI Data Security Standard Overview 5
PCI DSS Applicability Information 7
Relationship between PCI DSS and PA-DSS 9
Scope of Assessment for Compliance with PCI DSS Requirements 10
Network Segmentation 10
Wireless 11
Third Parties/Outsourcing 11
Sampling of Business Facilities/System Components 12
Compensating Controls 13
Instructions and Content for Report on Compliance 14
Report Content and Format 14
Revalidation of Open Items 17
PCI DSS Compliance – Completion Steps 18
Detailed PCI DSS Requirements and Security Assessment Procedures 19
Build and Maintain a Secure Network 20
Requirement 1: Install and maintain a firewall configuration to protect cardholder data 20
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 24
Protect Cardholder Data 28
Requirement 3: Protect stored cardholder data 28
Requirement 4: Encrypt transmission of cardholder data across open, public networks 35
Maintain a Vulnerability Management Program 37
Requirement 5: Use and regularly update anti-virus software or programs 37
Requirement 6: Develop and maintain secure systems and applications 38
Implement Strong Access Control Measures 44
Requirement 7: Restrict access to cardholder data by business need to know 44
Requirement 8: Assign a unique ID to each person with computer access 46
Requirement 9: Restrict physical access to cardholder data 51
Regularly Monitor and Test Networks 55
Requirement 10: Track and monitor all access to network resources and cardholder data 55

Copyright 2010 PCI Security Standards Council LLC

Requirement 11: Regularly test security systems and processes. 59
Maintain an Information Security Policy 64
Requirement 12: Maintain a policy that addresses information security for all personnel. 64
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers 70
Appendix B: Compensating Controls 72
Appendix C: Compensating Controls Worksheet 73
Compensating Controls Worksheet – Completed Example 74
Appendix D: Segmentation and Sampling of Business Facilities/System Components 75



Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. Below is a high-level overview of the 12 PCI DSS requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. The following sections provide detailed guidelines and best practices to assist entities prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS Requirements and Testing Procedures begin on **page 19.**

Copyright 2010 PCI Security Standards Council LLC

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources, including:

- Attestations of Compliance
- *Navigating PCI DSS: Understanding the Intent of the Requirements*
- The *PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms*
- Frequently Asked Questions (FAQs)
- Information Supplements and Guidelines

***Note**: Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements – they do not change, eliminate or supersede the PCI DSS or any of its requirements.*

Please refer to www.pcisecuritystandards.org for more information.

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Applicability Information

PCI DSS applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, as follows:

Cardholder Data includes:	*Sensitive Authentication Data includes:*
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full magnetic stripe data or equivalent on a chip ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply only to PAN.

PCI DSS represents a minimum set of control objectives which may be enhanced by local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name), or define an entity's disclosure practices related to consumer information. Examples include legislation related to consumer data protection, privacy, identity theft, or data security. PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

The following table illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

Copyright 2010 PCI Security Standards Council LLC

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS ***only applies*** if PANs are stored, processed and/or transmitted.

1 *Sensitive authentication data must not be stored after authorization (even if encrypted).*

2 *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

Copyright 2010 PCI Security Standards Council LLC

Relationship between PCI DSS and PA-DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor (per PA-DSS Requirement 13.1).

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *PCI DSS Requirements and Security Assessment Procedures* (this document). The PA-DSS details what a payment application must support to facilitate a customer's PCI DSS compliance.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), and PINs and PIN blocks, along with the damaging fraud resulting from these breaches.

Just a few of the ways payment applications can prevent compliance include:

- Storage of magnetic stripe data and/or equivalent data from the chip in the customer's network after authorization;
- Applications that require customers to disable other features required by the PCI DSS, like anti-virus software or firewalls, in order to get the payment application to work properly; and
- Vendors' use of unsecured methods to connect to the application to provide support to the customer.

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

Please note the following regarding PA-DSS applicability:

- PA-DSS ***does*** apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS ***does not*** apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For detailed guidance on determining whether PA-DSS applies to a given payment application, please refer to the PA-DSS Requirements and Security Assessment Procedures, which can be found at www.pcisecuritystandards.org.

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. "System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Appendix D: Segmentation and Sampling of Business Facilities/System Components provides more information on the effect of network segmentation and sampling on the scope of a PCI DSS assessment.

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (WLAN) is connected to, or part of, the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Third Parties/Outsourcing

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components in the cardholder data environment.

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the assessed entity and which apply to the service provider. There are two options for third-party service providers to validate compliance:

Copyright 2010 PCI Security Standards Council LLC

1) They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance; or
2) If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

See the bullet beginning "For managed service provider (MSP) reviews," in Item 3, "Details about Reviewed Environment," in the "Instructions and Content for Report on Compliance" section, below, for more information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

Sampling of Business Facilities/System Components

Sampling is not a PCI DSS requirement. However, after considering the overall scope and complexity of the environment being assessed, the assessor may independently select representative samples of business facilities/system components in order to assess PCI DSS requirements. These samples must be defined first for business facilities and then for system components within each selected business facility. Samples must be a representative selection of all of the types and locations of business facilities, as well as types of system components within selected business facilities. Samples must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Sampling of business facilities/system components for an assessment does not reduce the scope of the cardholder data environment or the applicability of PCI DSS requirements. Whether or not sampling is to be used, PCI DSS requirements apply to the entire cardholder data environment. If sampling is used, each sample must be assessed against all applicable PCI DSS requirements. Sampling of the PCI DSS Requirements themselves is not permitted.

Examples of business facilities include but are not limited to: corporate offices, stores, franchise locations, processing facilities, data centers, and other facility types in different locations. Sampling should include system components within each selected business facility. For example, for each business facility selected, include a variety of operating systems, functions, and applications that are applicable to the area under review.

As an example, the assessor may define a sample at a business facility to include Sun servers running Apache WWW, Windows servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single version of an OS (for example, Windows 7 or Solaris 10), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When independently selecting samples of business facilities/system components, assessors should consider the following:

- If there are standard, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that all business facilities/system components are configured per the standard processes.
- If there is more than one type of standard security and/or operational process in place (for example, for different types of business facilities/system components), the sample must be large enough to include business facilities/system components secured with each type of process.

Copyright 2010 PCI Security Standards Council LLC

- If there are no standard PCI DSS processes/controls in place and each business facility/system component is managed through non-standard processes, the sample must be larger for the assessor to be assured that each business facility/system component has implemented PCI DSS requirements appropriately.

For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size,
- Document and validate the standardized PCI DSS processes and controls used to determine sample size, and
- Explain how the sample is appropriate and representative of the overall population.

Please also refer to:
Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Assessors must revalidate the sampling rationale for each assessment. If sampling is to be used, different samples of business facilities and system components must be selected for each assessment.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet*.

For each and every compensating control, the Compensating Controls Worksheet *(Appendix C)* **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned *Appendices B* and *C* for more details on "compensating controls."

Copyright 2010 PCI Security Standards Council LLC



Instructions and Content for Report on Compliance

This document must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand to determine reporting requirements and instructions.

Report Content and Format

Follow these instructions for report content and format when completing a Report on Compliance:

1. **Executive Summary**

   Include the following:

   - Describe the entity's payment card business, including:
     - Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data

       Note: *This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.*
     - How they process payment (directly, indirectly, etc.)
     - What types of payment channels they serve, such as card-not-present (for example, mail-order-telephone-order (MOTO), e-Commerce), or card-present
     - Any entities that they connect to for payment transmission or processing, including processor relationships
   - A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:
     - Connections into and out of the network
     - Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
     - Other necessary payment components, as applicable

Copyright 2010 PCI Security Standards Council LLC

2. Description of Scope of Work and Approach Taken

Describe the scope, per the Scope of Assessment section of this document, including the following:

- Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:
  - The methods or processes used to identify and document all existences of cardholder data
  - How the results were evaluated and documented
  - How the effectiveness and accuracy of the methods used were verified
  - That the assessor validates that the scope of the assessment is accurate and appropriate.
- Environment on which assessment focused (for example, client's Internet access points, internal corporate network, processing connections)
- If network segmentation is in place and was used to reduce scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation
- If sampling is used during the assessment, for each sample set selected (of business facilities/system components) document the following:
  - Total population
  - Number sampled
  - Rationale for sample selected
  - Description of the standardized PCI DSS security and operational processes and controls used to determine sample size, and how the processes/controls were validated
  - How the sample is appropriate and representative of the overall population
  - Description of any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded
- List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any international entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to, or could impact the security of the cardholder data environment, and describe security in place for these wireless environments
- The version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment

Copyright 2010 PCI Security Standards Council LLC

3. **Details about Reviewed Environment**

   Include the following details in this section:

   - A diagram of each piece of the communication link, including LAN, WAN or Internet
   - Description of cardholder data environment, for example:
     - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback and other flows as applicable
     - List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):
       - List all of the elements of stored cardholder data
       - How data is secured
       - How access to data stores are logged
   - List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each
   - List of service providers and other third parties with which the entity shares cardholder data

     Note: *These entities are subject to PCI DSS Requirement 12.8.)*
   - List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's *PA-DSS Implementation Guide*.

     Note: *It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.)*
   - List of individuals interviewed, their organizations, titles, and topics covered
   - List of documentation reviewed
   - For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

Copyright 2010 PCI Security Standards Council LLC

4. **Contact Information and Report Date**

   Include:

   - Contact information for merchant or service provider and assessor
   - Timeframe of assessment---specify the duration and the time period over which the assessment occurred
   - Date of report

5. **Quarterly Scan Results**

   - Summarize the four most recent quarterly ASV scan results in the Executive Summary as well as in comments at Requirement 11.2.2.

     Note: *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies:*

     1) The most recent scan result was a passing scan,

     2) The entity has documented policies and procedures requiring quarterly scanning going forward, and

     3) Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.

     For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

   - Scan must cover all externally accessible (internet-facing) IP addresses in existence at the entity, in accordance with the *PCI Approved Scanning Vendors (ASV) Program Guide*.

6. **Findings and Observations**

   Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.

   All assessors *must:*

   - Use the Detailed PCI DSS Requirements and Security Assessment Procedures template to provide detailed report descriptions and findings on each requirement and sub-requirement.
   - Ensure that all N/A responses are clearly explained.
   - Review and document any compensating controls considered to conclude that a control is in place.

   See "Compensating Controls" section above and *Appendices B* and *C* for more details on compensating controls.

Revalidation of Open Items

A "controls in place" report is required to verify compliance. The report is considered non-compliant if it contains "open items," or items that will be finished at a future date. The merchant/service provider must address these items before validation is completed. After open items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions (see below).

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Compliance – Completion Steps

1. Complete the Report on Compliance (ROC) according to the section above entitled "Instructions and Content for Report on Compliance."
2. Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of passing scan(s) from the ASV.
3. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Attestations of Compliance are available on the PCI SSC website (www.pcisecuritystandards.org).
4. Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

Copyright 2010 PCI Security Standards Council LLC



Detailed PCI DSS Requirements and Security Assessment Procedures

For the *PCI DSS Requirements and Security Assessment Procedures*, the following defines the table column headings:

- **PCI DSS Requirements** – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements are "in place."
- **In Place** – This column must be used by the assessor to provide a brief description of the controls which were validated as "in place" for each requirement, including descriptions of controls found to be in place as a result of compensating controls, or as a result of a requirement being "Not Applicable."

  Note: *This column must not be used for controls that are not yet in place or for open items to be completed at a future date.*
- **Not in Place** – This column must be used by the assessor to provide a brief description of controls that are not in place. Note that a non-compliant report should not be submitted to a payment brand or acquirer unless specifically requested. , For further instructions on non-compliant reports, please refer to the Attestations of Compliance, available on the PCI SSC website (www.pcisecuritystandards.org).
- **Target Date/Comments** – For those controls "Not in Place" the assessor may include a target date that the merchant or service provider expects to have controls "in Place." Any additional notes or comments may be included here as well.

Copyright 2010 PCI Security Standards Council LLC



Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.			
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.			
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.			
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.			
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.			
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.			
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.			
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.			
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.			
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.			
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ.			
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)			
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.			
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* ▪ *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.			
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.			
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.			
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.			

Copyright 2010 PCI Security Standards Council LLC

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:			
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions			
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.			
	2.1.1.c Verify default passwords/passphrases on access points were changed.			
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.			
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.			
	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.			
	2.2.c Verify that system configuration standards are applied when new systems are configured.			
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).			
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.			
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.			
	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.			
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.			
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.			
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.			
	2.2.4.b. Verify enabled functions are documented and support secure configuration.			
	2.2.4.c. Verify that only documented functionality is present on the sampled system components.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following:			
	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.			
	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.			
	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.			
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*.	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.			

Copyright 2010 PCI Security Standards Council LLC



Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	**3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:			
3.1.1 Implement a data retention and disposal policy that includes: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	**3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).			
	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.			
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.			
	3.1.1.d Verify that policies and procedures include at least one of the following: A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.			
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: ***Note:*** *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.			
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.			
	3.2.c For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The cardholder's name* ▪ *Primary account number (PAN)* ▪ *Expiration date* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.*	**3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	**3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Several database schemas • Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***Notes:*** • *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* • *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads, with the pads being securely stored ▪ Strong cryptography, with associated key-management processes and procedures			
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).			
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.			
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.			
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).			
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).			
	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: ***Note:*** *This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.			
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.			
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.			
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data.			
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.			
	3.6.c Examine the key-management procedures and perform the following:			
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.			
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.			
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.			

Copyright 2010 PCI Security Standards Council LLC



PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.			
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.			
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.			
	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). ***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.			
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.			
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.			

Copyright 2010 PCI Security Standards Council LLC



Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* ▪ The Internet ▪ Wireless technologies, ▪ Global System for Mobile communications (GSM) ▪ General Packet Radio Service (GPRS).	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:			
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.			
	4.1.b Verify that only trusted keys and/or certificates are accepted.			
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.			
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)			
	4.1.e For SSL/TLS implementations: ▪ Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). ▪ Verify that no cardholder data is required when HTTPS does not appear in the URL.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.			
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.			
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.			

Copyright 2010 PCI Security Standards Council LLC



Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.			
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:			
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.			
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.			
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.			
	5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.			

Copyright 2010 PCI Security Standards Council LLC

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. ***Note:*** *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.			
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. ***Notes:*** • *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.* • *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High."			
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.			
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices.			
	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.			
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.			
	6.3.d From an examination of written software development processes, and interviews of software developers, verify that:			
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. ***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	**6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			
	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.			
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:			
6.4.1 Separate development/test and production environments	**6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation.			
6.4.2 Separation of duties between development/test and production environments	**6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.			
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3** Production data (live PANs) are not used for testing or development.			
6.4.4 Removal of test data and accounts before production systems become active	**6.4.4** Test data and accounts are removed before a production system becomes active.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.			
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:			
6.4.5.1 Documentation of impact.	**6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change.			
6.4.5.2 Documented change approval by authorized parties.	**6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.			
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.			
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.			
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.			
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:	**6.5.a** Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.			
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.			
Note: *The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	**6.5.c** Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)			
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)			
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)			
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)			
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)			
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). ***Note:*** *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.			
Note: *Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):*				
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)			
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)			
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: ▪ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: – At least annually – After any changes – By an organization that specializes in application security – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections ▪ Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. ***Note:*** *"An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*			

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:			
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.			
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).			
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.			
7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.			
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			
7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.			
7.2.3 Default "deny-all" setting ***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.			



Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.			
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: • Obtain and examine documentation describing the authentication method(s) used. • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.			
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.			
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.			
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: • Obtain and examine an authorization form for each ID. • Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.			
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.			
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.			
8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.			
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.			
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.			
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.			
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: ▪ Generic user IDs and accounts are disabled or removed ▪ Shared user IDs for system administration activities and other critical functions do not exist ▪ Shared and generic user IDs are not used to administer any system components			
	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.			
	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.			
	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non-consumer users are given guidance as to when, and under what circumstances, passwords must change.			
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.			
	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements.			
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.			
	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.			
	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.			
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.			
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	**8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access.			
	8.5.16.b Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).			
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.			
	8.5.16.d Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).			

Copyright 2010 PCI Security Standards Council LLC

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. ▪ Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. ▪ Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.			
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	**9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.			
	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.			
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.			
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.			
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	**9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following: ▪ Granting new badges, ▪ Changing access requirements, and ▪ Revoking terminated onsite personnel and expired visitor badges			
	9.2.b Verify that access to the badge system is limited to authorized personnel.			
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.			
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.			
	9.3.2.b Verify that visitor badges expire.			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.			

Copyright 2010 PCI Security Standards Council LLC



PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months.			
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5.a** Observe the storage location's physical security to confirm that backup media storage is secure.			
	9.5.b Verify that the storage location security is reviewed at least annually.			
9.6 Physically secure all media.	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).			
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.			
9.7.1 Classify media so the sensitivity of the data can be determined.	**9.7.1** Verify that all media is classified so the sensitivity of the data can be determined.			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.			
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.			
9.9 Maintain strict control over the storage and accessibility of media.	**9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.			
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:			
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.			
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).			

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.			
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.			
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.			
10.2.5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.			
10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.			
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.			
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.			
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.			
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.			
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.			
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.			
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.			
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	**10.4.a** Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.			
	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.			
	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.			
10.4.2 Time data is protected.	**10.4.2.a** Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.			
	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).			
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.			
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.			
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.			
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.			

Copyright 2010 PCI Security Standards Council LLC



PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.*	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.			
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.			
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.			

Copyright 2010 PCI Security Standards Council LLC

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.			
	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: ▪ WLAN cards inserted into system components ▪ Portable wireless devices connected to system components (for example, by USB, etc.) ▪ Wireless devices attached to a network port or network device			
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.			
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.			
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	**11.2** Verify that internal and external vulnerability scans are performed as follows:			
11.2.1 Perform quarterly internal vulnerability scans.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.			
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.			
	11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.*	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.			
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).			
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.			
11.2.3 Perform internal and external scans after any significant change. ***Note:*** *Scans conducted after changes may be performed by internal staff.*	**11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.			
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: ▪ For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS. ▪ For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.			
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.			
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.			
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.			
11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.			
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.			
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.			
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: ▪ System executables ▪ Application executables ▪ Configuration and parameter files ▪ Centrally stored, historical or archived, log and audit files			
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.			



Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).			
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.			
(Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.b** Review risk assessment documentation to verify that the risk assessment process is performed at least annually.			
12.1.3 Includes a review at least annually and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	**12.3** Obtain and examine the usage policies for critical technologies and perform the following:			
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies.			
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).			
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.			
12.3.4 Labeling of devices to determine owner, contact information and purpose	**12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.			
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.			
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.			
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products.			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.			
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4** Verify that information security policies clearly define information security responsibilities for all personnel.			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.			
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.			
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all personnel.			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).			
	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.			
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.			
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.			
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.			

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.			
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.			
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises ▪ Coverage and responses of all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands	**12.9.1.a** Verify that the incident response plan includes: ▪ Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum: ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) ▪ Coverage and responses for all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands			
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.			

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.			
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained.			
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.			
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			

Copyright 2010 PCI Security Standards Council LLC

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below:			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: No entity on the system can use a shared web server user ID. All CGI scripts used by an entity must be created and run as the entity's unique user ID.			

Copyright 2010 PCI Security Standards Council LLC

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).			
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) **Important:** An entity's files may not be shared by group.			
	A.1.2.c Verify that an entity's users do not have write access to shared system binaries.			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU			
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: Logs are enabled for common third-party applications. Logs are active by default. Logs are available for review by the owning entity. Log locations are clearly communicated to the owning entity.			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

Copyright 2010 PCI Security Standards Council LLC

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

Note: *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if: (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Copyright 2010 PCI Security Standards Council LLC

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

***Note:** Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. **Constraints**	List constraints precluding compliance with the original requirement.	
2. **Objective**	Define the objective of the original control; identify the objective met by the compensating control.	
3. **Identified Risk**	Identify any additional risk posed by the lack of the original control.	
4. **Definition of Compensating Controls**	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. **Validation of Compensating Controls**	Define how the compensating controls were validated and tested.	
6. **Maintenance**	Define process and controls in place to maintain compensating controls.	

Compensating Controls Worksheet – Completed Example

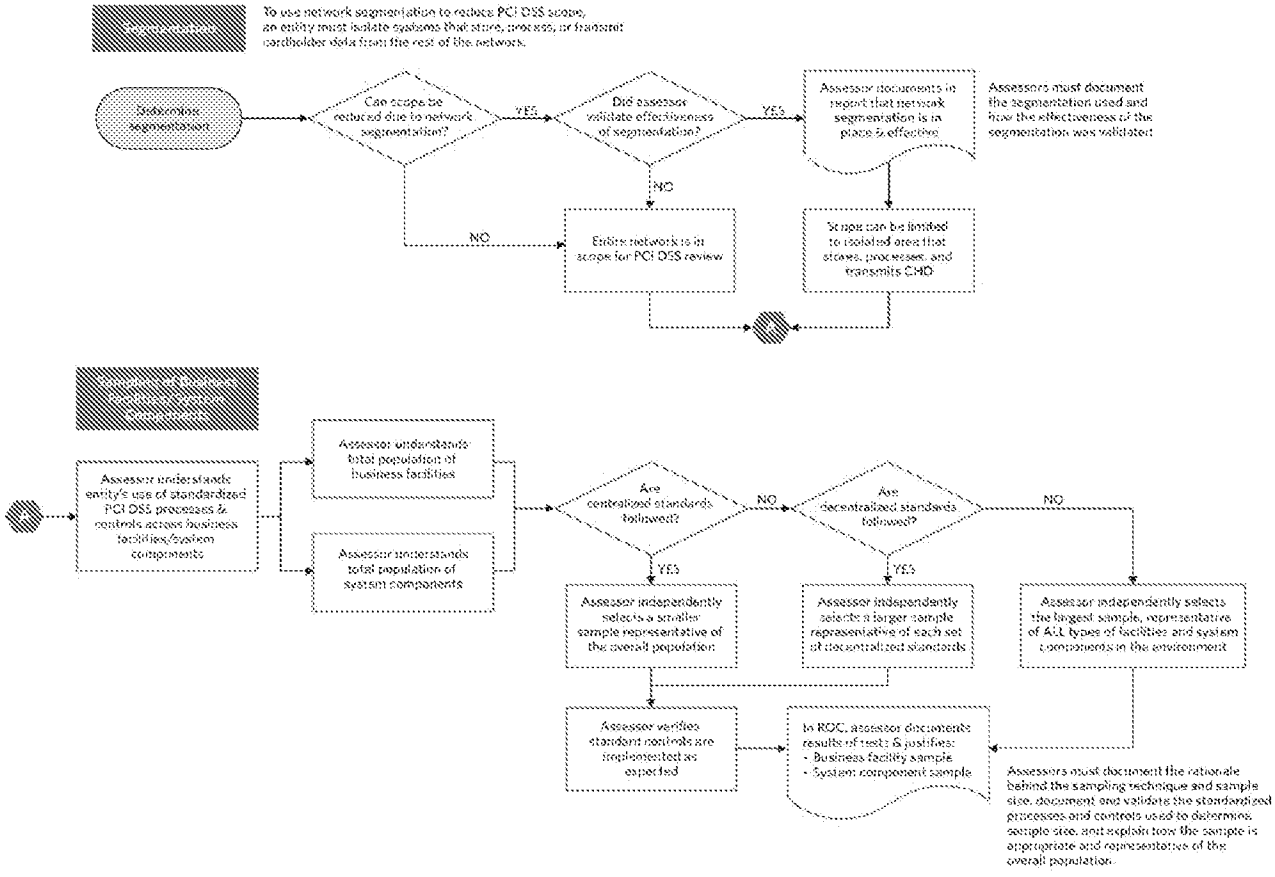
Use this worksheet to define compensating controls for any requirement noted as "in place" via compensating controls.

Requirement Number: *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. **Constraints**	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. **Objective**	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. **Identified Risk**	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. **Definition of Compensating Controls**	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.*
5. **Validation of Compensating Controls**	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges.*
6. **Maintenance**	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged.*

Copyright 2010 PCI Security Standards Council LLC

Appendix D: Segmentation and Sampling of Business Facilities/System Components



Appendix B

Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire A-EP and Attestation of Compliance

Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing

For use with PCI DSS Version 3.2.1

June 2018

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
N/A	1.0		Not used.
N/A	2.0		Not used.
February 2014	3.0		New SAQ to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data. Content aligns with PCI DSS v3.0 requirements and testing procedures.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1.*
June 2015	3.1		Update Requirement 11.3 to fix error.
July 2015	3.1	1.1	Updated to remove references to "best practices" prior to June 30, 2015, and remove the PCI DSS v2 reporting option for Requirement 11.3
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.* Requirements added from PCI DSS v3.2 Requirements 1, 5, 6, 7, 8, 10, 11, and Appendix A2.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Table of Contents

Document Changes i

Before You Begin iii

PCI DSS Self-Assessment Completion Steps iv

Understanding the Self-Assessment Questionnaire iv

Expected Testing iv

Completing the Self-Assessment Questionnaire v

Guidance for Non-Applicability of Certain, Specific Requirements v

Legal Exception v

Section 1: Assessment Information 1

Section 2: Self-Assessment Questionnaire A-EP 4

Build and Maintain a Secure Network 4

Requirement 1: Install and maintain a firewall configuration to protect data 4

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 8

Protect Cardholder Data 12

Requirement 3: Protect stored cardholder data 12

Requirement 4: Encrypt transmission of cardholder data across open, public networks 13

Maintain a Vulnerability Management Program 15

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs 15

Requirement 6: Develop and maintain secure systems and applications 17

Implement Strong Access Control Measures 23

Requirement 7: Restrict access to cardholder data by business need to know 23

Requirement 8: Identify and authenticate access to system components 24

Requirement 9: Restrict physical access to cardholder data 29

Regularly Monitor and Test Networks 31

Requirement 10: Track and monitor all access to network resources and cardholder data 31

Requirement 11: Regularly test security systems and processes 36

Maintain an Information Security Policy 41

Requirement 12: Maintain a policy that addresses information security for all personnel 41

Appendix A: Additional PCI DSS Requirements 44

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers 44

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS 44

Appendix A3: Designated Entities Supplemental Validation (DESV) 44

Appendix B: Compensating Controls Worksheet 45

Appendix C: Explanation of Non-Applicability 46

Section 3: Validation and Attestation Details 47

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Before You Begin

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process, or transmit any cardholder data on their systems or premises.

SAQ A-EP merchants confirm that, for this payment channel:

- Your company accepts only e-commerce transactions;
- All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

This SAQ is applicable only to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Note: *For the purposes of this SAQ, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s). This is because the merchant website directly impacts how the payment card data is transmitted, even though the website itself does not receive cardholder data.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Self-Assessment Completion Steps

1. Identify the applicable SAQ for your environment—refer to the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website for information.
2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using (as defined in Part 2g of the Attestation of Compliance).
3. Assess your environment for compliance with applicable PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1 (Parts 1 & 2 of the AOC) – Assessment Information and Executive Summary.
   - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ A-EP)
   - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
5. Submit the SAQ and Attestation of Compliance (AOC), along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand or other requester.

Understanding the Self-Assessment Questionnaire

The questions contained in the "PCI DSS Question" column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS *(PCI Data Security Standard Requirements and Security Assessment Procedures)*	▪ Guidance on Scoping ▪ Guidance on the intent of all PCI DSS Requirements ▪ Details of testing procedures ▪ Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	▪ Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*. Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. ***Only one response should be selected for each question.***

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. (See *Guidance for Non-Applicability of Certain, Specific Requirements* below for examples.) All responses in this column require a supporting explanation in Appendix C of the SAQ.

Guidance for Non-Applicability of Certain, Specific Requirements

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:			DBA (doing business as):		
Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ Others (please specify):		

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary *(continued)*

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation.)*	☐ Yes ☐ No

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	☐ Yes ☐ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☐ Yes ☐ No

If Yes:

Name of service provider:	**Description of services provided:**

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Eligibility to Complete SAQ A-EP

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☐	Merchant accepts only e-commerce transactions;
☐	All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
☐	Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
☐	If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
☐	Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
☐	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☐	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☐	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Self-Assessment Questionnaire A-EP

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document.*

Self-assessment completion date:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
1.1	Are firewall and router configuration standards established and implemented to include the following:					
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	• Review documented process. • Interview personnel. • Examine network configurations.	☐	☐	☐	☐
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	• Review current network diagram. • Examine network configurations.	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	• Interview responsible personnel.	☐	☐	☐	☐
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	• Review current dataflow diagram. • Examine network configurations.	☐	☐	☐	☐
	(b) Is there a process to ensure the diagram is kept current?	• Interview personnel.	☐	☐	☐	☐
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	• Review firewall configuration standards. • Observe network configurations to verify that a firewall(s) is in place.	☐	☐	☐	☐
	(b) Is the current network diagram consistent with the firewall configuration standards?	• Compare firewall configuration standards to current network diagram.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
1.1.6	(a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?	• Review firewall and router configuration standards.	☐	☐	☐	☐
	(b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?	• Review firewall and router configuration standards. • Examine firewall and router configurations.	☐	☐	☐	☐
1.1.7	(a) Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	• Review firewall and router configuration standards.	☐	☐	☐	☐
	(b) Are firewall and router rule sets reviewed at least every six months?	• Examine documentation from firewall reviews.	☐	☐	☐	☐
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows: ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*					
1.2.1	(a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	• Review firewall and router configuration standards. • Examine firewall and router configurations.	☐	☐	☐	☐
	(b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	• Review firewall and router configuration standards. • Examine firewall and router configurations.	☐	☐	☐	☐
1.2.2	Are router configuration files secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?	• Review firewall and router configuration standards. • Examine router configuration files and router configurations.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	• Review firewall and router configuration standards. • Examine firewall and router configurations.	☐	☐	☐	☐
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:					
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	• Examine firewall and router configurations.	☐	☐	☐	☐
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	• Examine firewall and router configurations.	☐	☐	☐	☐
1.3.3	Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network? (For example, block traffic originating from the internet with an internal address)	• Examine firewall and router configurations.	☐	☐	☐	☐
1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	• Examine firewall and router configurations.	☐	☐	☐	☐
1.3.5	Are only established connections permitted into the network?	• Examine firewall and router configurations.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
1.3.7	(a) Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet? ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* *Internal use of RFC1918 address space instead of registered addresses.*	• Examine firewall and router configurations.	☐	☐	☐	☐
	(b) Is any disclosure of private IP addresses and routing information to external entities authorized?	• Examine firewall and router configurations. • Interview personnel.	☐	☐	☐	☐
1.4	(a) Is personal firewall software (or equivalent functionality) installed and active on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE?	• Review policies and configuration standards. • Examine mobile and/or employee-owned devices.	☐	☐	☐	☐
	(b) Is the personal firewall software (or equivalent functionality) configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?	• Review policies and configuration standards. • Examine mobile and/or employee-owned devices.	☐	☐	☐	☐
1.5	Are security policies and operational procedures for managing firewalls: • Documented • In use • Known to all affected parties?	• Review security policies and operational procedures. • Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network? *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).*	▪ Review policies and procedures. ▪ Examine vendor documentation. ▪ Observe system configurations and account settings. ▪ Interview personnel.	☐	☐	☐	☐
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	▪ Review policies and procedures. ▪ Review vendor documentation. ▪ Examine system configurations and account settings. ▪ Interview personnel.	☐	☐	☐	☐
2.2	(a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards? *Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).*	▪ Review system configuration standards. ▪ Review industry-accepted hardening standards. ▪ Review policies and procedures. ▪ Interview personnel.	☐	☐	☐	☐
	(b) Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	▪ Review policies and procedures. ▪ Interview personnel.	☐	☐	☐	☐
	(c) Are system configuration standards applied when new systems are configured?	▪ Review policies and procedures. ▪ Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
2.2 *(cont.)*	(d) Do system configuration standards include all of the following: – Changing of all vendor-supplied defaults and elimination of unnecessary default accounts? – Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server? – Enabling only necessary services, protocols, daemons, etc., as required for the function of the system? – Implementing additional security features for any required services, protocols or daemons that are considered to be insecure? – Configuring system security parameters to prevent misuse? – Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?	• Review system configuration standards.	☐	☐	☐	☐
2.2.1	(a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server? *For example, web servers, database servers, and DNS should be implemented on separate servers.*	• Examine system configurations.	☐	☐	☐	☐
	(b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	• Examine system configurations.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	▪ Review configuration standards. ▪ Examine system configurations.	☐	☐	☐	☐
	(b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	▪ Review configuration standards. ▪ Interview personnel. ▪ Examine configuration settings. ▪ Compare enabled services, etc. to documented justifications.	☐	☐	☐	☐
2.2.3	Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?	▪ Review configuration standards. ▪ Examine configuration settings.	☐	☐	☐	☐
2.2.4	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	▪ Interview personnel.	☐	☐	☐	☐
	(b) Are common system security parameters settings included in the system configuration standards?	▪ Review system configuration standards.	☐	☐	☐	☐
	(c) Are security parameter settings set appropriately on system components?	▪ Examine system components. ▪ Examine security parameter settings. ▪ Compare settings to system configuration standards.	☐	☐	☐	☐
2.2.5	(a) Has all unnecessary functionality---such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	▪ Examine security parameters on system components.	☐	☐	☐	☐
	(b) Are enabled functions documented and do they support secure configuration?	▪ Review documentation. ▪ Examine security parameters on system components.	☐	☐	☐	☐
	(c) Is only documented functionality present on system components?	▪ Review documentation. ▪ Examine security parameters on system components.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
2.3	Is non-console administrative access encrypted as follows:					
	(a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	▪ Examine system components. ▪ Examine system configurations. ▪ Observe an administrator log on.	☐	☐	☐	☐
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	▪ Examine system components. ▪ Examine services and files.	☐	☐	☐	☐
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	▪ Examine system components. ▪ Observe an administrator log on.	☐	☐	☐	☐
	(d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	▪ Examine system components. ▪ Review vendor documentation. ▪ Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
3.2	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	• Review policies and procedures. • Examine system configurations. • Examine deletion processes.	☐	☐	☐	☐
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):					
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	• Examine data sources including: – Incoming transaction data – All logs – History files – Trace files – Database schema – Database contents	☐	☐	☐	☐
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	• Examine data sources including: – Incoming transaction data – All logs – History files – Trace files – Database schema – Database contents	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

	PCI DSS Question	Expected Testing	Response (Check one response for each question) Yes	Yes with CCW	No	N/A
4.1	(a) Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks? ***Note:*** *Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).*	• Review documented standards. • Review policies and procedures. • Review all locations where CHD is transmitted or received. • Examine system configurations.	☐	☐	☐	☐
	(b) Are only trusted keys and/or certificates accepted?	• Observe inbound and outbound transmissions. • Examine keys and certificates.	☐	☐	☐	☐
	(c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	• Examine system configurations.	☐	☐	☐	☐
	(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	• Review vendor documentation. • Examine system configurations.	☐	☐	☐	☐
	(e) For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received? *For example, for browser-based implementations:* • *"HTTPS" appears as the browser Universal Record Locator (URL) protocol, and* • *Cardholder data is only requested if "HTTPS" appears as part of the URL.*	• Examine system configurations.	☐	☐	☐	☐
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	• Review policies and procedures.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
4.3	Are security policies and operational procedures for encrypting transmissions of cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures. ▪ Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	• Examine system configurations.	☐	☐	☐	☐
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	• Review vendor documentation. • Examine system configurations.	☐	☐	☐	☐
5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	• Interview personnel.	☐	☐	☐	☐
5.2	Are all anti-virus mechanisms maintained as follows:					
	(a) Are all anti-virus software and definitions kept current?	• Examine policies and procedures. • Examine anti-virus configurations, including the master installation. • Examine system components.	☐	☐	☐	☐
	(b) Are automatic updates and periodic scans enabled and being performed?	• Examine anti-virus configurations, including the master installation. • Examine system components.	☐	☐	☐	☐
	(c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	• Examine anti-virus configurations. • Review log retention processes.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
5.3	Are all anti-virus mechanisms: ▪ Actively running? ▪ Unable to be disabled or altered by users? ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	▪ Examine anti-virus configurations. ▪ Examine system components. ▪ Observe processes. ▪ Interview personnel.	☐	☐	☐	☐
5.4	Are security policies and operational procedures for protecting systems against malware: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures. ▪ Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.1	Is there a process to identify security vulnerabilities, including the following: ▪ Using reputable outside sources for vulnerability information? ▪ Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities? ***Note**: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.*	▪ Review policies and procedures. ▪ Interview personnel. ▪ Observe processes.	☐	☐	☐	☐
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	▪ Review policies and procedures.	☐	☐	☐	☐
	(b) Are critical security patches installed within one month of release? ***Note**: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	▪ Review policies and procedures. ▪ Examine system components. ▪ Compare list of security patches installed to recent vendor patch lists.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.4.5	(a) Are change-control procedures documented and require the following? – Documentation of impact – Documented change control approval by authorized parties – Functionality testing to verify that the change does not adversely impact the security of the system – Back-out procedures	• Review change control processes and procedures.	☐	☐	☐	☐
	(b) Are the following performed and documented for all changes:					
6.4.5.1	Documentation of impact?	• Trace changes to change control documentation. • Examine change control documentation.	☐	☐	☐	☐
6.4.5.2	Documented approval by authorized parties?	• Trace changes to change control documentation. • Examine change control documentation.	☐	☐	☐	☐
6.4.5.3	(a) Functionality testing to verify that the change does not adversely impact the security of the system?	• Trace changes to change control documentation. • Examine change control documentation.	☐	☐	☐	☐
	(b) For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?	• Trace changes to change control documentation. • Examine change control documentation.	☐	☐	☐	☐
6.4.5.4	Back-out procedures?	• Trace changes to change control documentation. • Examine change control documentation.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.4.6	Upon completion of a significant change, are all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable?	• Trace changes to change control documentation. • Examine change control documentation. • Interview personnel. • Observe affected systems or networks.	☐	☐	☐	☐
6.5	Do software-development processes address common coding vulnerabilities?	• Review software-development policies and procedures.	☐	☐	☐	☐
	Are developers trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities?	• Examine software-development policies and procedures. • Examine training records.	☐	☐	☐	☐
	(c) Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:					
6.5.1	Do coding techniques address injection flaws, particularly SQL injection? *Note: Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.*	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.2	Do coding techniques address buffer overflow vulnerabilities?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.4	Do coding techniques address insecure communications?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.5	Do coding techniques address improper error handling?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.6	Do coding techniques address all "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
For web applications and application interfaces (internal or external), are applications developed based on secure coding guidelines to protect applications from the following additional vulnerabilities:					
6.5.7 Do coding techniques address cross-site scripting (XSS) vulnerabilities?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.8 Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.9 Do coding techniques address cross-site request forgery (CSRF)?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐
6.5.10 Do coding techniques address broken authentication and session management?	• Examine software-development policies and procedures. • Interview responsible personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.6	For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying *either* of the following methods? • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: – At least annually – After any changes – By an organization that specializes in application security – That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* **– OR –** • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows: – Is situated in front of public-facing web applications to detect and prevent web-based attacks. – Is actively running and up to date as applicable. – Is generating audit logs. – Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	• Review documented processes. • Interview personnel. • Examine records of application security assessments. • Examine system configuration settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
6.7	Are security policies and operational procedures for developing and maintaining secure systems and applications: • Documented • In use • Known to all affected parties?	• Review security policies and operational procedures. • Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:					
7.1.2	Is access to privileged user IDs restricted as follows: ▪ To least privileges necessary to perform job responsibilities? ▪ Assigned only to roles that specifically require that privileged access?	▪ Examine written access control policy. ▪ Interview personnel. ▪ Interview management. ▪ Review privileged user IDs.	☐	☐	☐	☐
7.1.3	Is access assigned based on individual personnel's job classification and function?	▪ Examine written access control policy. ▪ Interview management. ▪ Review user IDs.	☐	☐	☐	☐
7.1.4	Is documented approval by authorized parties required, specifying required privileges?	▪ Review user IDs. ▪ Compare with documented approvals. ▪ Compare assigned privileges with documented approvals.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1	Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:					
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	• Review password procedures. • Interview personnel.	☐	☐	☐	☐
8.1.2	Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled such that user IDs are implemented only as authorized (including with specified privileges)?	• Review password procedures. • Examine privileged and general user IDs and associated authorizations. • Observe system settings.	☐	☐	☐	☐
8.1.3	Is access for any terminated users immediately deactivated or removed?	• Review password procedures. • Examine terminated users accounts. • Review current access lists. • Observe returned physical authentication devices.	☐	☐	☐	☐
8.1.4	Are inactive user accounts either removed or disabled within 90 days?	• Review password procedures. • Observe user accounts.	☐	☐	☐	☐
8.1.5	(a) Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	• Review password procedures. • Interview personnel. • Observe processes.	☐	☐	☐	☐
	(b) Are third-party remote access accounts monitored when in use?	• Interview personnel. • Observe processes.	☐	☐	☐	☐
8.1.6	(a) Are repeated access attempts limited by locking out the user ID after no more than six attempts?	• Review password procedures. • Examine system configuration settings.	☐	☐	☐	☐
8.1.7	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?	• Review password procedures. • Examine system configuration settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.1.8	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	• Review password procedures. • Examine system configuration settings.	☐	☐	☐	☐
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	• Review password procedures. • Observe authentication processes.	☐	☐	☐	☐
8.2.1	(a) Is strong cryptography used to render all authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components?	• Review password procedures. • Review vendor documentation. • Examine system configuration settings. • Observe password files. • Observe data transmissions.	☐	☐	☐	☐
8.2.2	Is user identity verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)?	• Review authentication procedures. • Observe personnel.	☐	☐	☐	☐
8.2.3	(a) Are user password parameters configured to require passwords/passphrases meet the following? – A minimum password length of at least seven characters – Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	• Examine system configuration settings to verify password parameters.	☐	☐	☐	☐
8.2.4	(a) Are user passwords/passphrases changed at least once every 90 days?	• Review password procedures. • Examine system configuration settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.2.5	(a) Must an individual submit a new password/phrase that is different from any of the last four passwords/passphrases he or she has used?	• Review password procedures. • Sample system components. • Examine system configuration settings.	☐	☐	☐	☐
8.2.6	Are passwords/passphrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?	• Review password procedures. • Examine system configuration settings. • Observe security personnel.	☐	☐	☐	☐
8.3	Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication, as follows: ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*					
8.3.1	Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access?	• Examine system configurations. • Observe administrator logging into CDE.	☐	☐	☐	☐
8.3.2	Is multi-factor authentication incorporated for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network?	• Examine system configurations. • Observe personnel connecting remotely.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.4	(a) Are authentication policies and procedures documented and communicated to all users?	• Review policies and procedures. • Review distribution method. • Interview personnel. • Interview users.	☐	☐	☐	☐
	(b) Do authentication policies and procedures include the following? – Guidance on selecting strong authentication credentials – Guidance for how users should protect their authentication credentials – Instructions not to reuse previously used passwords – Instructions that users should change passwords if there is any suspicion the password could be compromised	• Review policies and procedures. • Review documentation provided to users.	☐	☐	☐	☐
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components?	• Review policies and procedures. • Examine user ID lists. • Interview personnel.	☐	☐	☐	☐
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), is the use of these mechanisms assigned as follows? • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	• Review policies and procedures. • Interview personnel. • Examine system configuration settings and/or physical controls.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
8.8	Are security policies and operational procedures for identification and authentication: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Examine security policies and operational procedures. ▪ Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9: Restrict physical access to cardholder data

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	• Observe physical access controls. • Observe personnel.	☐	☐	☐	☐
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	• Review policies and procedures for physically securing media. • Interview personnel.	☐	☐	☐	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	• Review policies and procedures for distribution of media.	☐	☐	☐	☐
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	• Review policies and procedures for media classification. • Interview security personnel.	☐	☐	☐	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	• Interview personnel. • Examine media distribution tracking logs and documentation.	☐	☐	☐	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	• Interview personnel. • Examine media distribution tracking logs and documentation.	☐	☐	☐	☐
9.7	Is strict control maintained over the storage and accessibility of media?	• Review policies and procedures.	☐	☐	☐	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	• Review periodic media destruction policies and procedures.	☐	☐	☐	☐
	(c) Is media destruction performed as follows:					

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	▪ Review periodic media destruction policies and procedures. ▪ Interview personnel. ▪ Observe processes.	☐	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	▪ Examine security of storage containers.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.1	Are audit trails enabled and active for system components?	▪ Observe processes. ▪ Interview system administrator.	☐	☐	☐	☐
	Is access to system components linked to individual users?	▪ Observe processes. ▪ Interview system administrator.	☐	☐	☐	☐
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:					
10.2.2	All actions taken by any individual with root or administrative privileges?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐
10.2.3	Access to all audit trails?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐
10.2.4	Invalid logical access attempts?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐
10.2.5	Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐
10.2.6	Initialization, stopping, or pausing of the audit logs?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐
10.2.7	Creation and deletion of system-level objects?	▪ Interview personnel. ▪ Observe audit logs. ▪ Examine audit log settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.3	Are the following audit trail entries recorded for all system components for each event:					
10.3.1	User identification?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.3.2	Type of event?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.3.3	Date and time?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.3.4	Success or failure indication?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.3.5	Origination of event?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.3.6	Identity or name of affected data, system component, or resource?	• Interview personnel. • Observe audit logs. • Examine audit log settings.	☐	☐	☐	☐
10.4	Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current? ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	• Review time configuration standards and processes.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.4.1	Are the following processes implemented for critical systems to have the correct and consistent time:					
	(a) Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?	• Review time configuration standards and processes. • Examine time-related system parameters.	☐	☐	☐	☐
	(b) Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?	• Review time configuration standards and processes. • Examine time-related system parameters.	☐	☐	☐	☐
	(c) Do systems receive time only from designated central time server(s)?	• Review time configuration standards and processes. • Examine time-related system parameters.	☐	☐	☐	☐
10.4.2	Is time data is protected as follows: (a) Is access to time data restricted to only personnel with a business need to access time data?	• Examine system configurations and time-synchronization settings.	☐	☐	☐	☐
	(b) Are changes to time settings on critical systems logged, monitored, and reviewed?	• Examine system configurations and time-synchronization settings and logs.	☐	☐	☐	☐
10.4.3	Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock). *Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).*	• Examine system configurations.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.5	Are audit trails secured so they cannot be altered, as follows:					
10.5.1	Is viewing of audit trails limited to those with a job-related need?	▪ Interview system administrators ▪ Examine system configurations and permissions	☐	☐	☐	☐
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	▪ Interview system administrators. ▪ Examine system configurations and permissions.	☐	☐	☐	☐
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	▪ Interview system administrators. ▪ Examine system configurations and permissions.	☐	☐	☐	☐
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?	▪ Interview system administrators. ▪ Examine system configurations and permissions.	☐	☐	☐	☐
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	▪ Examine settings, monitored files, and results from monitoring activities.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows? ***Note:*** *Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.*					
10.6.1	(b) Are the following logs and security events reviewed at least daily, either manually or via log tools? – All security events – Logs of all system components that store, process, or transmit CHD and/or SAD – Logs of all critical system components – Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	• Review security policies and procedures. • Observe processes. • Interview personnel.	☐	☐	☐	☐
10.6.2	(b) Are logs of all other system components periodically reviewed---either manually or via log tools—based on the organization's policies and risk management strategy?	• Review security policies and procedures. • Review risk assessment documentation. • Interview personnel.	☐	☐	☐	☐
10.6.3	(b) Is follow up to exceptions and anomalies identified during the review process performed?	• Review security policies and procedures. • Observe processes. • Interview personnel.	☐	☐	☐	☐
10.7	(b) Are audit logs retained for at least one year?	• Review security policies and procedures. • Interview personnel. • Examine audit logs.	☐	☐	☐	☐
	(c) Are at least the last three months' logs immediately available for analysis?	• Interview personnel. • Observe processes.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 11: Regularly test security systems and processes

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.2.2	(a) Are quarterly external vulnerability scans performed? ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	• Review results from the four most recent quarters of external vulnerability scans.	☐	☐	☐	☐
	(b) Do external quarterly scan and rescan results satisfy the *ASV Program Guide* requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	• Review results of each external quarterly scan and rescan.	☐	☐	☐	☐
	(c) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV?	• Review results of each external quarterly scan and rescan.	☐	☐	☐	☐
11.2.3	(a) Are internal and external scans, and rescans as needed, performed after any significant change? ***Note:*** *Scans must be performed by qualified personnel.*	• Examine and correlate change control documentation and scan reports.	☐	☐	☐	☐
	(b) Does the scan process include rescans until: – For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS; – For internal scans, a passing result is obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	• Review scan reports.	☐	☐	☐	☐
	(c) Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	• Interview personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.3	Does the penetration-testing methodology include the following? • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results	• Examine penetration-testing methodology. • Interview responsible personnel.	☐	☐	☐	☐
11.3.1	(a) Is *external* penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	• Examine scope of work. • Examine results from the most recent external penetration test.	☐	☐	☐	☐
	(b) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	• Interview responsible personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	• Examine penetration testing results.	☐	☐	☐	☐
11.3.4	If segmentation is used to isolate the CDE from other networks:					
	(a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE?	• Examine segmentation controls. • Review penetration-testing methodology.	☐	☐	☐	☐
	(b) Does penetration testing to verify segmentation controls meet the following? – Performed at least annually and after any changes to segmentation controls/methods. – Covers all segmentation controls/methods in use. – Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	• Examine results from the most recent penetration test.	☐	☐	☐	☐
	(c) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	• Interview responsible personnel.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.4	(a) Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: – At the perimeter of the cardholder data environment, and – At critical points in the cardholder data environment.	• Examine system configurations. • Examine network diagrams.	☐	☐	☐	☐
	(b) Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?	• Examine system configurations. • Interview responsible personnel.	☐	☐	☐	☐
	(c) Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	• Examine IDS/IPS configurations. • Examine vendor documentation.	☐	☐	☐	☐
11.5	(a) Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files? *Examples of files that should be monitored include:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log, and audit files* • *Additional critical files determined by entity (for example, through risk assessment or other means)*	• Observe system settings and monitored files. • Examine system configuration settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
11.5 *(cont.)*	(b) Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? ***Note:*** *For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).*	• Observe system settings and monitored files. • Review results from monitoring activities.	☐	☐	☐	☐
11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	• Examine system configuration settings.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	• Review the information security policy.	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	• Review the information security policy. • Interview responsible personnel.	☐	☐	☐	☐
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	• Review information security policy and procedures. • Interview a sample of responsible personnel.	☐	☐	☐	☐
12.5	(b) Are the following information security management responsibilities formally assigned to an individual or team:					
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	• Review information security policy and procedures.	☐	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	• Review security awareness program.	☐	☐	☐	☐
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:					
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?	• Review policies and procedures. • Observe processes. • Review list of service providers.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	▪ Observe written agreements. ▪ Review policies and procedures.	☐	☐	☐	☐
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	☐	☐	☐	☐
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	☐	☐	☐	☐
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	• Review the incident response plan. • Review incident response plan procedures.	☐	☐	☐	☐
	(b) Does the plan address the following, at a minimum:					
	– Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Specific incident response procedures?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Business recovery and continuity procedures?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Data backup processes?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Analysis of legal requirements for reporting compromises?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Coverage and responses of all critical system components?	• Review incident response plan procedures.	☐	☐	☐	☐
	– Reference or inclusion of incident response procedures from the payment brands?	• Review incident response plan procedures.	☐	☐	☐	☐

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
A2.1	*For POS POI terminals **(at the merchant or payment-acceptance location)** using SSL and/or early TLS:* Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS? ***Note:** This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.*	• Review documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS.	☐	☐	☐	☐

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. **Constraints**	List constraints precluding compliance with the original requirement.	
2. **Objective**	Define the objective of the original control; identify the objective met by the compensating control.	
3. **Identified Risk**	Identify any additional risk posed by the lack of the original control.	
4. **Definition of Compensating Controls**	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. **Validation of Compensating Controls**	Define how the compensating controls were validated and tested.	
6. **Maintenance**	Define process and controls in place to maintain compensating controls.	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A-EP (Section 2), dated *(SAQ completion date)*.

Based on the results documented in the SAQ A-EP noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (***check one):***

☐	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☐	PCI DSS Self-Assessment Questionnaire A-EP, Version *(version of SAQ)*, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☐	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3. PCI DSS Validation *(continued)*

Part 3a. Acknowledgement of Status (continued)

☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *(ASV Name)*

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	*Date:*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data.	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☐	☐	
3	Protect stored cardholder data.	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks.	☐	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs.	☐	☐	
6	Develop and maintain secure systems and applications.	☐	☐	
7	Restrict access to cardholder data by business need to know.	☐	☐	
8	Identify and authenticate access to system components.	☐	☐	
9	Restrict physical access to cardholder data.	☐	☐	
10	Track and monitor all access to network resources and cardholder data.	☐	☐	
11	Regularly test security systems and processes.	☐	☐	
12	Maintain a policy that addresses information security for all personnel.	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.	☐	☐	

** PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
16/535,424	**01/05/2023 09:47:17 PM ET**	**124452.00122**

Title of Invention

Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	2047	FILED BY	Tami Day
PATENT CENTER #	61396304	FILING DATE	08/08/2019
CUSTOMER #	27557	FIRST NAMED INVENTOR	Robert Evan POLLIN
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Jonathan King

Documents

TOTAL DOCUMENTS: 3

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
Amendment-.pdf		167	-	1896 KB
Amendment--A....pdf	(1-1)	1	Amendment/Request for Reconsideration-After Non-Final Rejection	90 KB
Amendment--CLM.pdf	(2-12)	11	Claims	108 KB
Amendment--REM.pdf	(13-167)	155	Applicant Arguments/Remarks Made in an Amendment	1874 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Amendment-.pdf	1F8E1F0CF092C3C4E3606FB6CCA16AB46D9D994F20D9CB108552BB97E21D8838A9B8765D6D3AC6426CD517E377499AA6EA261F250996EE964C4FC03E05051954
Amendment--A....pdf	3434C581E5DBC5DFEF522F923F7BD6A77D310AF180BA6011F2D81C004FE5AE5A96C5F9CFB3B176814F3CF623D9F92340859B3635D923C2B7825D13DCC3D40C75
Amendment--CLM.pdf	F1785474D0F19ABBDA739D13D696C48503D2DDFD1AB2D1F6006466D00AFE4A547483AC279A32B273FA814F259EF4E31048166CCDA3EA2C2877FB0CC7C1D0516C
Amendment--REM.pdf	5DBCDF0AD3106EEB9D4C75F94A54DB89512FE554CF86995A0782A13D876341689EB14DAF3BF6EE372507D5FB0C649CF9E5E6AFD2FFCF0A36DB1DC4C4842BDA3B

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
16/535,424	01/05/2023 09:47:17 PM ET	124452.00122

Title of Invention

Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	2047	FILED BY	Tami Day
PATENT CENTER #	61396304	AUTHORIZED BY	Jonathan King
CUSTOMER #	27557	FILING DATE	08/08/2019
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Robert Evan POLLIN

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
DA / 501922	E202315L48152537	Tami Day

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
501922	37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.19 (Document supply fees); 37 CFR 1.20 (Post issuance fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2201	EACH INDEPENDENT CLAIM IN EXCESS OF THREE	192.00	2	384.00
			TOTAL AMOUNT:	$384.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/535,424	Filing Date 08/08/2019	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $230 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	01/05/2023	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 37	Minus	** 45	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0		x $192 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/BURNELL L ROSS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

27557 7590 10/05/2022

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER	
AZIZ, ABDULMAJEED	
ART UNIT	**PAPER NUMBER**
3695	
NOTIFICATION DATE	**DELIVERY MODE**
10/05/2022	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

WashingtonDocketing@blankrome.com
jyeddo@BlankRome.com

Office Action Summary	Application No. 16/535,424	Applicant(s) POLLIN et al.	
	Examiner ABDULMAJEED AZIZ	Art Unit 3695	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 4/11/22.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-7,9-22,24-35 and 37-47 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-7,9-22,24-35 and 37-47 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8/8/19 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. **Claims 1-7, 9-22, 24-35 & 37-47** are currently pending and have been examined in this application. This NON-FINAL communication is in response to the amendment submitted on 4/11/22.

2. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/11/22 has been entered.

Response to Arguments

4. Applicant's arguments filed regarding **101** have been fully considered but they are not persuasive.

Issue #1

Applicant: A. The claimed invention improves the functioning of the prior art merchant server itself by eliminating the need for that merchant server to include numerous components and to perform numerous computer processing steps required by the PCI Data Security Standard Claims that "purport to improve the functioning of the computer itself' are patent eligible under § 101.10 In Enfish, for example, the Federal Circuit held that claims directed to a "self- referential" table were patent eligible because the self-referential table allowed for faster searching of data, allowed for more effective storage of data other than structured text, and allowed more flexibility in configuring the database." To process payments **prior to the claimed invention, prior art merchant systems were required to receive, store, and transmit cardholder data**. Therefore, as described in paragraphs [0004]-[0005] of the instant specification, prior art merchant systems were required to comply with Payment Card Industry (PCI) Data Security Standards. The PCI Data Security Standard that was in place on the effective filing date of the present application" is attached as Appendix A. The claimed invention **eliminates the need for merchant servers to receive, store, and transmit cardholder data by allowing those merchant servers to outsource the processing of cardholder data to the secure server**. As a result, the claimed invention eliminates the need for that merchant

server to comply with the PCI Data Security Standard of Appendix A. Instead, in the years since the claimed invention has become available, the Payment Card Industry Security Standards Council has published requirements applicable to "e-commerce merchants with a website(s) that does not itself receive cardholder data,"3 which are attached as Appendix B. The PCI Data Security Standard of Appendix B is applicable to "e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties," meaning "All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor." As described below, the PCI Data Security Standard of Appendix B does not require that merchant systems that outsource the processing of cardholder data to the secure server recited in the claims include a number of computer components or perform a number a computer processing steps that were required of prior art merchant systems that received cardholder data. Additionally, if any of the requirements of the PCI Data Security Standard of Appendix B are not applicable, that PCI Data Security Standard allows those merchants to simply indicate that those requirements are not applicable.[15] Meanwhile, as described below, **several requirements of the PCI Data Security Standard of Appendix B are not applicable to merchant systems that outsource the processing of cardholder data to the secure server recited in the claims**. Therefore, just like the self-referential table at issue in Enfish improved the functioning of the computer itself, the claimed invention improves the functioning of the merchant server itself by eliminating the need for that merchant server to include the following components and to perform the following computer processing. Prior to the claimed invention, **prior art merchant systems were required to protect stored cardholder data by** rendering any primary account number

(PAN) unreadable anywhere it is stored[16] by one-way hashing the entire PAN **using strong cryptography**, using index tokens and securely stored pads, or using strong cryptography with associated key-management processes and procedures. Prior art merchant systems were required to generate strong data-encrypting cryptographic keys, encrypt those data-encrypting cryptographic keys using key-encrypting cryptographic keys, store the key-encrypting cryptographic keys separately from the data- encrypting cryptographic keys, and securely distribute the data-encrypting cryptographic keys. Prior art merchant systems were required to change cryptographic keys that had reached the end of their cryptoperiod (e.g., after a defined period of time and/or a defined amount of ciphertext had been produced).[22] Prior art merchant systems were also required to include functionality to retire or replace cryptographic keys when required,[23] for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key).[24] Prior art **merchant systems were also required to mask PAN** when displayed.[25]

If the prior art merchant system used disk encryption,[26] the prior art merchant system was required to manage logical access independently of native operating system access control mechanisms.[27] A prior art merchant system was **not compliant with the PCI Data Security Standard i**f it used local user account databases or **tied decryption keys to user accounts**.28 If the prior art merchant system used manual clear-text cryptographic key management operations, the prior art merchant system was required to provide functionality to manage those operations using split knowledge and dual control.[29] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key. To avoid the requirement to conduct quarterly

manual reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy, a prior art **merchant system was required to include a programmatic process to automatically remove stored cardholder data** exceeding the requirements defined in the merchant's data retention policy. Except in limited circumstances,[32] prior art merchant systems were required to perform a process to securely delete sensitive authentication data received from cardholders, including the full contents of any magnetic stripe or chip,[33] any card validation code,[34] and any personal identification number (PIN) or encrypted PIN block.[35] While merchant systems that partially outsource their e-commerce payment channel using the claimed invention are still required to securely delete any sensitive authentication data they receive,[36] **the claimed invention allows merchant systems to process payments without receiving any sensitive authentication data**. Prior art merchant systems were required to use strong cryptography and security protocols to safeguard sensitive cardholder data transmitted over open, public networks such as the Internet, wireless networks, and mobile networks.[37] The PCI Data Security Standard suggested using SSL/TLS, IPSEC, or SSH to transmit sensitive cardholder data over open, public networks.[38] Prior art merchant systems were required to accept only trusted cryptographic keys and/or certificates,[39] to use a protocol implemented to use only secure configurations (that did not support insecure versions or configurations),[40] and to use "the proper encryption strength" (according to vendor recommendations/best practices) for the encryption methodology in use.[41] Prior art merchant systems were required to render PAN unreadable or secured with strong cryptography whenever sent to end-user messaging technologies such as email, instant messaging, or chat programs.[42] Again, merchants who partially outsource their e-commerce payment channel using

the claimed invention are still required to safeguard any sensitive cardholder data they transmit.[43] However, the claimed invention allows merchant systems to process payments without transmitting any sensitive cardholder data. Wireless networks transmitting cardholder data or connected to the cardholder data environment were required to use industry best practices to implement strong encryption for authentication or transmission.[44] The PCI Data Security Standard noted that the use of Wired Equivalent Privacy (WEP) as a security control was prohibited and suggested IEEE 802.1 li as an example of industry best practices.[45] Note that the IEEE 802.1 li standard makes use of the Advanced Encryption Standard (AES) block cipher, which requires a dedicated chip that was not commonly included in most wireless network hardware.

Examiner: The use of tokenization and applying the concept of tokenization to a particular server that outsources what the merchant server could have done to process a payment does not go beyond the 'apply-it' standard. Applicant's comparisons of the claims of the instant case with those of Enfish are not persuasive. In Enfish, the claims describe the steps of configuring a computer memory in accordance with a self-referential table. On the other hand the claims of the instant case employ a generic computer system comprising a memory and a generic processor with suitable programming to perform the claimed functions. The claims in the instant application are applying computers to a problem rooted in abstract idea. There are no improvements to another technology or technical field, no improvements to the functioning of the computer itself, transformation or reduction of a particular article to a different state or thing or any other meaningful limitations beyond what is mentioned in the rejection below

using the claimed system. The claimed sequence of steps comprises only "conventional steps, specified at a high level of generality," which is insufficient to supply an "inventive concept." Id. at 2357 (quoting Mayo, 132 S. Ct. at 1294, 1297, 1300). Also the addition of merely novel or non-routine components to the claimed idea does not necessarily turn an abstraction into something concrete (See Ultramercial, Inc. v. Hulu, LLC, _ F.3d __, 2014 WL 5904902, (Fed. Cir. Nov. 14, 2014).

Issue #2

Applicant: B. Additionally, because the secure server recited in the claims can perform cardholder data functions for multiple merchant servers, the claimed invention improves the functioning of the combined system for processing payments (i.e., both the merchant servers and the secure server) by eliminating redundant computer components and redundant processing steps - The claimed invention **allows multiple merchant systems to outsource the processing of cardholder data to the secure server recited in the claims while maintaining PCI compliance** as described in the PCI Data Security Standard of Appendix B. Accordingly, rather than each merchant system being required to include the required computer components, only the secure server is required to include many of the computer components required by the PCI Data Security Standard of Appendix A. Additionally, rather than each merchant system being required to perform each of the software processing steps required by the PCI Data Security Standard of Appendix A, many of those software processing steps are only required to be performed once by the secure server recited in the claims for each of those merchant systems to maintain PCI compliance. When providing functionality for payers of multiple merchants to

provide PAN (e.g., via an application programming interface (API) or a secure connection via the internet, such as a redirect URL or a widget or window within a website provided by the merchant server), the secure server can provide a single interface that masks that PAN when displayed,[51] a single process to remove stored cardholder data exceeding the requirements defined in the secure system's data retention policy,[52] and a single process to securely delete sensitive authentication data. The secure system can protect that cardholder data for all of those merchant systems by generating strong data-encrypting cryptographic keys, encrypting those data-encrypting cryptographic keys using key-encrypting cryptographic keys, securely storing the cryptographic keys, and retiring or replacing the cryptographic keys when required. One particularly beneficial improvement provided by the claimed invention is the **secure system can perform a single key rotation process and ensure that all cryptographic keys used for all merchants are changed before they reach the end of their cryptoperiod**. While receiving and transmitting sensitive cardholder data for multiple merchants, the secure server recited in the claims only requires one set of components that uses strong cryptography and security protocols to safeguard that sensitive cardholder data during transmission over open, public networks[56] (including wireless network hardware with the dedicated chip[7] required by the IEEE 802.1 li standard[58] if needed to transmit cardholder data wirelessly).

Examiner: Outsourcing the processing to another device does not meaningfully reduce the processing that needs to occur in maintaining PCI compliance. Similar to above, it does not go beyond the apply-it standard. Where is the **technical problem** described **in the specification** as

well as the **technical solution**, and where are said technical elements **mapped to in the claim** language?

Issue #3

Applicant: C. Processing a payment, by a server, is a technical process - In addition to improvements to computer functionality, the subject matter eligibility guidelines recognize that "an improvement to other technology or technical field" may integrate a judicial exception into a practical application under Prong Two of Step 2A or recite "significantly more" than an instruction to apply the judicial exception under Step 2B. In BASCOM, the claims were directed to filtering content on the internet.59 As described in BASCOM, prior art content filtering methods included installing filtering software on each local computer.60 However, it was "difficult and time consuming to install" that software "on every end-user's client machine."61 Other prior art m^{et}hods included relocating the filtering software to a local server or an ISP.62 However, those "o^{ne}-size-fits-all" solutions were not ideal because "a single set of filtering criteria is often not appropriate for all of the end-users."63 Therefore, the claims at issue in BASCOM provided individually customizable filtering at the remote ISP server.64 The ISP stored customized filtering mechanisms for different users, required each user to log in, and applied the filtering mechanisms associated with each user.65 The Federal Circuit noted that, when viewed individually, the claimed components ("local client computer," "remote ISP server," "Internet computer network," and "controlled access network accounts") were described in the specification as well-known, generic computer components.66 Meanwhile, the specification stated that "the filtering scheme" performed by those components "can be any of a number of

known-schemes, or hybrids thereof."67 However, the Federal Circuit held that the claims were patent eligible under § 101 because the "particular arrangement of elements" was "a technical improvement over prior art ways of filtering such content." Installing a filtering tool at a location remote from the end-users, with customizable filtering features specific to each end user, gave that filtering tool both the benefits of a filter on a local computer and the benefits of a filter on the ISP server.[68] The court also noted that the claims do not "preempt all ways of filtering content on the Internet" but "rather, they recite a specific, discrete implementation of the abstract idea of filtering content. " In DDR Holdings, the claims were directed to constructing and serving a hybrid web page that merges content associated with the products of the third-party merchant with stored "visually perceptible elements" from a host website. There, the specific issue was that, "upon the click of an advertisement for a third-party product displayed on a host's website, the host website would lose that visitor as he or she is "transported to the third party's website." To solve that problem, the claims were directed to "an automatically-generated hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website related to the clicked advertisement" so that, "rather than instantly losing visitors to the third-party's website, the host website can instead send its visitors to a web page on the outsource provider's server that 1) incorporates 'look and feel' elements from the host website, and 2) provides visitors with the opportunity to purchase products from the third- party merchant without actually entering that merchant's website." The Federal Circuit held that such claims were patent eligible "because they do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the

Internet" and instead provided a claimed solution that was "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." The court also noted that the claims "do not attempt to preempt every application of the idea of increasing sales by making two web pages look the same," but rather "recite a specific way to automate the creation of a composite web page by an 'outsource provider' that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet." In both instances, the Federal Circuit held that the claims improved a technical process. As explained by the court in BASCOM: Although the invention in DDR's patent was engineered in the context of retaining potential customers, the invention was not claiming a business method per se, but was instead claiming a technical way to satisfy an existing problem for website hosts and viewers. Similarly, although the invention in the '606 patent [at issue in BASCOM] is engineered in the context of filtering content, the invention is not claiming the idea of filtering content simply applied to the Internet. The '606 patent is instead claiming a technology-based solution (not an abstract-idea-based solution implemented with generic technical components in a conventional way) to filter content on the Internet that overcomes existing problems with other Internet filtering systems. By taking a prior art filter solution (one-size-fits-all filter at the ISP server) and making it more dynamic and efficient (providing individualized filtering at the ISP server), the claimed invention represents a software-based invention that improves the performance of the computer system itself.75

Similarly, the claims at issue are directed to the technical process of processing a payment using a server**. While the invention is used in service of a business transaction, the claims are not directed to the process of marketing or arranging that business transaction, but rather to the**

technical process of receiving, safeguarding, and transmitting cardholder data while complying with the PCI Data Security Standard. As described in the instant specification (e.g., with reference to FIGS. 4a through 41), receiving and transmitting cardholder data is a technical process. Meanwhile, as described in exhausting detail in Sections A and B above, complying with the PCI Data Security Standard to safeguard that cardholder data requires specific computer components and the performance of specific computer processing steps.

Examiner: The argument is not persuasive. Regarding Bascom, applicant argues a non-conventional and non-generic arrangement. The BASCOM court agreed that the additional elements were generic computer, network, and Internet components that did not amount to significantly more when considered individually, but explained that the district court erred by failing to recognize that when combined, an inventive concept may be found in the non-conventional and non-generic arrangement of the additional elements, i.e., the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user (note that the term "inventive concept" is often used by the courts to describe additional element(s) that amount to significantly more than a judicial exception). In BASCOM, as discussed in the specification, the one-size-fits-all filter on the local server was not ideal because “a single set of filtering criteria is often not appropriate for all of the end-users.” By taking a prior art filter solution (one-size-fits-all filter at the ISP server) and making it more dynamic and efficient (providing individualized filtering at the ISP server), the claimed invention in BASCOM represented a “software- based invention[ ] that improve[s] the performance of the computer system itself.” The specification in the instant application does

not similarly describe technological problems with a technological solution. Instead, the specification describes a recognized business problem with a solution in the computer arts where a server is used to process information and perform computationally-intensive analysis for other locations (See 0004-0005 "Underlying software applications may require substantial modifications to achieve compliance, and significant changes in organizational structure and operating procedures may also be required. Thus, the time, effort, and cost required for merchants and processors to obtain PCI certification to receive and use credit card data are substantial"). Looking at the limitations in the instant application as an ordered combination adds nothing that is not already present when looking at the elements taken individually. There is no indication that the combination of elements improves the functioning of a computer or improves any other technology. Their collective functions merely provide conventional computer implementation. **How is this invention like Bascom?**

Issue #4

Applicant: D. The claimed invention improves the prior art process of processing a payment by eliminating the need for merchants to integrate their systems with the components required for PCI compliance - Prior to the claimed invention, merchants were required to integrate their systems with the computer components required for PCI compliance described in Sections A and B above, while ensuring that those components did not negatively impact the functions performed by the merchant system, including the user experience provided to their customers. **By enabling those merchants to outsource the processing of cardholder data to the secure server recited in the claims, the secure server and merchant server recited in the**

claims form a hybrid system (similar to the hybrid webpage[76] at issue in DDR[77]) that enables merchants to focus their efforts on their own core systems - and the user experience provided to their customers - while maintaining compliance with the PCI Data Security Standard of Appendix B.

Examiner: As far as the comparison to DDR is concerned, the patent at issue in DDR provided and Internet-based solution to solve a problem unique to the Internet (the problem in DDR Holdings (conventional Internet hyperlink protocol preventing websites from retaining visitors), that (1) did not foreclose other ways of solving the problem, and (2) recited a specific series of steps that resulted in a departure from the routine and conventional sequence of steps after the click of a hyperlink advertisement. In the instant invention, the claimed solution is not necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer" analysis. Id. Claim 1 generically requires “supervised machine learning”. It’s not clear how the generic recitations of a basic computer implementation/components integrates the judicial exception as to “impose[] a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception.” Guidance, 84 Fed. Reg. at 53. The applicant does not indicate that the operations of Claim 1 invoke any assertedly inventive programming, require any specialized computer hardware or other inventive computer components, i.e., a particular machine, or that the claimed invention is implemented using other than generic computer components to perform generic computer functions. See DDR Holdings, LLC v. Hotels.com, L.P., 773 F.3d 1245.

Issue #5

Applicant: E. Additionally, the claimed invention improves the prior art process of processing a payment by eliminating the need for each merchant to perform numerous tasks to comply with the PCI Data Security Standard - As described above, the Federal Circuit in BASCOM held that filtering content at the ISP server (rather than on each end-user's client machine) was patent eligible under § 101 because it eliminated the "difficult and time consuming" process of installing software "on every end-user's client machine." In addition to the required computer components and computer processing steps outlined in Sections A and B above, the PCI Data Security Standard also required that employees or agents of merchants using prior art merchant systems perform all of the tasks outlined in detail below. By providing functionality for multiple merchants to outsource the processing of cardholder data, the claimed invention improves the prior art process of processing a payment by eliminating the need for each merchant to individually perform those tasks. Therefore, **just like BASCOM's process of filtering internet content by an ISP server (rather than on each end-user's client machine) improved the prior art internet content filtering processes, outsourcing the receipt, storage, and processing of cardholder data from each merchant's system to the secure server recited in the claims improved the prior art payment processing process by eliminating the need for each merchant to each perform all of those tasks.** Prior to the claimed invention, merchants using prior art merchant systems were required to verify that the prior art merchant systems complied with each and every one of the requirements above. To protect stored cardholder

data, merchants were required to implement data retention and disposal policies, procedures, and processes to keep cardholder data storage to a minimum.[79] To comply with the PCI Data Security Standard, the data retention and disposal policy was required to limit data storage and retention time "to that which is required for legal, regulatory, and business requirements."[0] Merchants were required to have specific retention requirements for all cardholder data"[1] specifying the time period that cardholder data needed to be stored and the legal, regulatory, or business reason why that cardholder data needed to be stored for that time period.[82] The data retention and disposal policy was also required to include provisions for secure disposal of data (including disposal of cardholder data) when no longer needed for those legal, regulatory, or business reasons.[83] If the merchant system did not include the programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy, the merchant was required to conduct quarterly reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy. Merchants were required to examine data sources - including incoming transaction data, all logs (e.g., transaction logs, history logs, debugging logs, and error logs), history files, trace files, several database schemas, and database contents - to verify that the full contents of magnetic stripes or chips,[85] card validation codes,[86] and PINs or encrypted PIN blocks[87] were not stored under any circumstance. To verify that displayed PAN was masked, merchants were required to obtain and examine writing policies and examine displays of PAN (e.g., on screen or on paper receipts) to verify that the PAN was masked[88] and examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[89] To verify that stored PAN was rendered unreadable,

merchants were required to examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[90] Additionally, merchants were required to confirm that PAN was rendered unreadable by examining several tables or files from a sample of data repositories,[91] a sample of removable media (e.g., back-up tapes),[92] and a sample of audit logs.[93] To protect cryptographic keys, merchants were required to document and implement key- management processes and procedures.[94] The key-management processes and procedures were required to restrict access to the fewest number of custodians necessary[95] and to store cryptographic keys in the fewest possible locations and forms.[96] Merchants were required to periodically change cryptographic keys once they reached the end of their cryptoperiod (for example, as after a defined period of time had passed and/or after a defined amount of cipher- text had been produced) as defined by the associated application vendor or key owner and based on industry best practices and guidelines (e.g., NIST Special Publication 800-57).97 Merchants were also required to retire or replace cryptographic keys if the cryptographic key was suspected of being compromised[98] or when the integrity of the cryptographic key had been weakened (for example, if an employee with knowledge of a clear-text cryptographic key left the organization), for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key). If the merchant system used manual clear-text cryptographic key management operations, the merchant was required to manage those operations using split knowledge and dual control.[101] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key.[102] The merchant key-management procedures were

required to prevent unauthorize substitution of cryptographic keys.[103] Merchants were required to obtain written or electronic acknowledgement from all custodians of the cryptographic keys that those custodians understood and accepted their key- custodian responsibilities. [104] Merchants were required to observe a sample of transactions as they occurred to verify that cardholder data was encrypted during transit.[105] For SSL/TLS implementations, merchants were required to verify that HTTPS appeared as a part of the browser Universal Record Locator (URL) and that no cardholder data was required when HTTPS does not appear in the URL.[106] Merchants were also required to maintain a policy stating that unprotected PANs were not to be sent via end-user messaging technologies.

Examiner: See responses to Issue #1-3.

Issue #6

Applicant: F. The specific processing steps recited in the claims are not "extra-solution activity" and the Patent Office provides no evidence that those processing steps were so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement of 35 U.S.C. § 112(a) To support a factual determination that claimed features were "well-understood, routine, conventional activity," the subject matter eligibility guidelines require factual evidence that the specific "combination"[108] of elements recited in the claims were so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement

of 35 U.S.C. § 112(a).[109] The pending Office Action provides no evidence that the specific processing steps recited in the claims performed by the secure server recited in the claims are known, let alone so "widely prevalent" that they did not need description in a patent specification. The Interview Summary states that "the additional insignificant extra solution activity amount only to data gathering and data storing that are recognized by courts as well-understood routine conventional." First, the term "extra-solution activity" refers to "activities incidental to the primary process or product that are merely a nominal or tangential addition to the claim."110 Here, the claimed processing steps are not "incidental to the primary process" or "merely a nominal or tangential addition to the claim." Instead, performing those processing steps by the secure server (thereby outsourcing the processing of cardholder data) differentiates the claimed invention from a conventional transaction where a payer provides financial account information directly to the merchant server. Second, courts have not held that performing the specific "combination" of features recited in the claims - a secure server receiving an electronically-generated payment transaction instruction from a merchant server, establishing a secure connection via the internet with a computing system used by the payer to receive financial account information provided by the payer, receiving the financial account information provided by the payer via the secure connection, providing an electronic data token (representing the financial account information provided by the payer) to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer, storing the financial account information provided by the payer, and processing the payment using the financial account information provided by the payer - are well-understood, routine or conventional.

Examiner: Per the 101 rejection below, the claims do not recite significantly more. It's not clear how the solution overcomes the "apply-it" standard regarded in the rejection (applicant points to the well-known and conventional WURC standard, which the Examiner did not apply in the rejection).

No Prior Art rejection

5. **Claims 1-7, 9-22, 24-35 & 37-47** overcome 35 U.S.C. 102/103 for the following reasons:

Based on prior art search results, the prior art of record neither anticipates nor renders obvious the claimed subject matter, as a whole or taken in combination, and does not teach:

> **establishing a secure connection via the internet between the secure server and a computing system used by the payer to receive financial account information provided by the payer; receiving the financial account information provided by the payer via the secure connection;**

The closest prior art of record includes:

Tieken (US 20110161233) provides a method for providing secure transactions that include receiving an identifier of a financial account at a payment processor system (secure server).

Fleishman (US 20040148252) provides a person-to-person (P2P) payment platform and identity management system which facilitates online banking by allowing consumers to send and receive money in real-time, with no special registration outside of the users' existing banking relationship, and under the security, brand and control of their own respective banks.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Issued Patents

7. Claims **1-7, 9-22, 24-35 & 37-47** are rejected on the ground of nonstatutory double patenting as being unpatentable over Claims 1-26 of U.S. Patent No. 10423940 or '940 (15/408185). Although the claims at issue are not identical, they are not patentably distinct

from each other because the claims of the instant application are taught by the intervening claims associated with patent ('940).

Claim 31. (instant application)

'940 teaches the following limitations:

> **A method of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising: receiving enrollment data identifying a payer;**
>
> ('940 – [Claim 1])
>
> **generating an electronic instruction for a secure server that includes at least one data element associated with the payer,**
>
> ('940 – [Claim 1])
>
> **the electronic instruction requesting the establishment of a secure connection via the internet between the secure server and a computing system used by the payer for the secure server to**

('940 – [Claim 4])

receive financial account information provided by the payer;

('940 – [Claim 1])

outputting the electronic instruction to a communications network for transmittal to the secure server;

('940 – [Claim 1])

receiving, from the secure server, an electronic data token representing financial account information received by the secure server via the secure connection, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

('940 – [Claim 1])

storing the electronic data token in association with the enrollment data identifying the payer; and

('940 – [Claim 1])

processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and

('940 – [Claim 1])

instructs a payment processing system having access to the financial account information represented by the electronic data token.

('940 – [Claim 1])

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. **Claims 1-7, 9-22, 24-35 & 37-47** are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more.

The claims are either directed to a system or method, which is one of the statutory categories of invention. (*Step 1: YES*).

The Examiner has identified method **Claim 31** as the claim that represents the claimed invention for analysis and is similar to system **Claims 46** and method/system **(Claim 1 & 16)**. **Claim 31** recites the limitations of (**additional elements** emphasized in **bold** and are considered to be parsed from the remaining abstract idea):

A method of enrolling a payer by a merchant **server** operated by or for the benefit of a payee, the method comprising: receiving enrollment data identifying a payer; generating an **electronic** instruction for a secure **server** that includes at least one data element associated with the

payer, the **electronic** instruction requesting the establishment of a **secure connection** via the **internet** between the secure **server** and **a computing system** used by the payer for the secure **server** to receive financial account information provided by the payer; outputting the **electronic** instruction to **a communications network** for transmittal to the secure **server**; receiving, from the secure **server**, an **electronic** data token representing financial account information received by the secure **server** via the **secure connection**, wherein the merchant server does not receive the financial account information represented by the **electronic** data token and the secure **server** does not provide the **electronic** data token to the payer; storing the **electronic** data token in association with the enrollment data identifying the payer; and processing a payment from the payer by **electronically** generating a payment transaction instruction that includes a representation of the **electronic** data token and instructs a **payment processing system** having access to the financial account information represented by the **electronic** data token.

---

which is a process that, under its broadest reasonable interpretation, covers performance of the limitation(s) as a **Certain method of organizing human activity (fundamental economic practice** or **commercial or legal interaction**) of **processing a payment from a payer to a payee**.

If a claim limitation, under its broadest reasonable interpretation (BRI), covers performance of the limitation as a certain method of a **fundamental economic practice**

or **commercial or legal interaction**, then it falls within the "**Certain Methods of Organizing Human Activity**" grouping of abstract ideas.

Accordingly, the claim recites an abstract idea. (*Step 2A-Prong 1: YES. The claims are abstract)*

This judicial exception is not integrated into a practical application. Limitations that are *not* indicative of integration into a practical application include: (1) Adding the words "apply it" (or an equivalent) with the judicial exception, or mere instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea (MPEP 2106.05.f), (2) Adding insignificant extra-solution activity to the judicial exception (MPEP 2106.05.g), (3) Generally linking the use of the judicial exception to a particular technological environment or field of use (MPEP 2106.05.h). The **servers, secure connection via the internet, computing system, communications network and payment processing system** in **Claim 31** (as well as **processors, memory** of **Claim 16** and the processors, **non-transitory CRM** of **Claim 46**) are just using generic computer components. The computer hardware is recited at a high-level of generality (*i.e.*, as a generic processor performing a generic computer function) such that it amounts to **no more than mere instructions to implement an abstract idea by adding the words "apply it" (or an equivalent) with the judicial exception.** Accordingly, these additional elements, when considered separately and as an ordered combination, do not integrate the abstract idea into a practical application because they do not impose any meaningful limits on practicing the abstract idea. Therefore **claim 31** is directed to an abstract idea without a practical application. (*Step 2A-Prong 2: NO. The additional claimed elements are not integrated into a practical application*)

The claims do not include additional elements that are sufficient to amount to significantly more than the judicial exception because, when considered separately and as an ordered combination, they do not add significantly more (also known as an "inventive concept") to the exception. As discussed above with respect to integration of the abstract idea into a practical application, the additional element of using computer hardware amounts to **no more than mere instructions to implement an abstract idea by adding the words "apply it" (or an equivalent) with the judicial exception.** Mere instructions to implement an abstract idea on or with the use of generic computer components, cannot provide an inventive concept - rendering the claim patent ineligible. Thus **claim 31** is not patent eligible. (St*ep 2B: NO. The claims do not provide significantly more*)

The dependent claims further define the abstract idea that is present in their respective independent claims and hence are abstract for at least the reasons presented above. The dependent claims do not include any additional elements (**including Claim 4, 19 & 33 - API/ website – which is just a computer tool used to further implement the abstract idea; Claims 6, 21 & 34 – API/ website – which is just a computer tool used to further implement the abstract idea; Claims 9, 24, 37 & 47 – widget – a computer tool used to implement the abstract idea; Claim 10/11, 25/26, 38/39 – URL – which is just a form of data representation; Claim 12, 27, 40 – synchronous secure connection – which further implements the abstract idea using generic computer components**) that integrate the abstract idea into a practical application or are sufficient to amount to significantly more than the judicial exception when considered both individually and as an ordered combination. Therefore, the dependent claims are directed to an abstract idea. Thus, the aforementioned claims are not patent-eligible.

Conclusion

10. The prior art made of record, and not relied upon, considered pertinent to applicant' s disclosure or directed to the state of art is listed on the enclosed PTO-892.

11. The following is a brief description for relevant prior art that was cited but not applied:

Hammad (US 20120259782) provides a method for authenticating a cardholder using multiple tokenization authentication.

Hammad (US 20120136796) provides a method of enrolling a mobile device in a program that provides the mobile device with the ability to conduct card-present transactions.

Stringfellow (US 20120030066) provides a payment system that processes payment authorization requests for payment transactions to be conducted via a data communications network on behalf of online merchants, and is particularly, but not exclusively, suited to the processing of orders placed by financial instrument holders.

Moore (US 20100235286) provides a method and system for generating tokens in a transaction handling system.

Basu (US 9342832) provides a method for securing external systems with account token substitution.

Yanni (US 20040098350) provides a framework and system for purchasing of goods and services.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULMAJEED AZIZ whose telephone number is (571)270-5046. The examiner can normally be reached M-F 7-4:00 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ryan Donlon can be reached on 571-270-3602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for

information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABDULMAJEED AZIZ/

Primary Examiner, Art Unit 3695

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner ABDULMAJEED AZIZ	Art Unit 3695	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20110161233-A1	06-2011	Tieken; Craig A.	G06Q20/04	705/76
*	B	US-20120030066-A1	02-2012	Stringfellow; Westley	G06Q20/204	705/26.41
*	C	US-20040148252-A1	07-2004	Fleishman, Jack	G06Q20/223	705/39
*	D	US-20100235286-A1	09-2010	Moore; Daryl Richard	G06Q20/3821	705/26.1
*	E	US-20120136796-A1	05-2012	Hammad; Ayman	G06Q20/385	705/67
*	F	US-20120259782-A1	10-2012	Hammad; Ayman	G06Q20/3674	705/44
*	G	US-9342832-B2	05-2016	Basu; Gourab	G06Q20/385	1/1
*	H	US-20040098350-A1	05-2004	Labrou, Yannis	G06Q20/12	705/64
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	16535424	Filing Date	2019-08-08	Docket Number (if applicable)	124452-00122	Art Unit	3696
First Named Inventor	Robert Evan Pollin			Examiner Name	MACCAGANO, Pierre L.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 232185

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Michael C. Greenbaum/	Date (YYYY-MM-DD)	2022-04-11
Name	Michael C. Greenbaum	Registration Number	28419

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	45439653
Application Number:	16535424
International Application Number:	
Confirmation Number:	2047
Title of Invention:	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System
First Named Inventor/Applicant Name:	Robert Evan POLLIN
Customer Number:	27557
Filer:	Michael C. Greenbaum/Crystal Corsey
Filer Authorized By:	Michael C. Greenbaum
Attorney Docket Number:	124452.00122
Receipt Date:	11-APR-2022
Filing Date:	08-AUG-2019
Time Stamp:	11:26:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$790
RAM confirmation Number	E20224AB27072282
Deposit Account	022555
Authorized User	Crystal Corsey

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	20220411_RCE.pdf	1667155 cb8ee561a191092f800187e6cab31b603644d975	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of Continued Prosecution Application (CPA)/Request for Continued Examination(RCE)	20220411_Response_RCE.pdf	208861 579218e0d10882b5cb3bd41b87196bdb618d25d3	no	28
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	40791 3764dfcce9338004458 09ab3f173adacb84dd70d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1916807		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: 124452.00122
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert Evan POLLIN et al.

Application No.: 16/535,424 | Confirmation No.: 2047

Filed: August 8, 2019 | Art Unit: 3696

For: ENROLLING A PAYER BY A MERCHANT SERVER OPERATED BY OR FOR THE BENEFIT OF A PAYEE AND PROCESSING A PAYMENT FROM THE PAYER BY A SECURE SERVER | Examiner: Pierre L. MACCAGNO

RESPONSE TO FINAL REJECTION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Final Office Action dated December 10, 2021, the Applicant respectfully submits the following together with a Request for Continued Examination:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS

1. (Currently Amended): A method of processing a payment from a payer to a payee, the method being performed by a secure server, the method comprising:

receiving an electronically-generated payment transaction instruction from a merchant server, the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee;

establishing ~~a communications link with the payer~~ a secure connection via the internet between the secure server and a computing system used by the payer to receive financial account information provided by the payer;

receiving the financial account information provided by the payer via the ~~communications link~~ secure connection;

providing an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;

storing the financial account information provided by the payer;

processing the payment using the financial account information provided by the payer; and

forwarding at least a portion of the payment to the payee.

2. (Previously Presented): The method of claim 1, further comprising:

receiving a second payment transaction instruction from the merchant server, the second payment transaction instruction including a representation of the electronic data token and specifying the amount of the second payment from the payer to the payee;

processing the second payment using the financial account information represented by the electronic data token; and

forwarding at least a portion of the second payment to the payee.

3. (Previously Presented): The method of claim 2, wherein the representation of the electronic data token is the electronic data token.

4. (Previously Presented): The method of claim 1, wherein the payment transaction instruction is generated by the merchant server using an application programming interface provided to the merchant server by the secure server.

5. (Previously Presented): The method of claim 4, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server.

6. (Previously Presented): The method of claim 4, wherein the application programming interface is implemented within a website hosted by the merchant server.

7. (Previously Presented): The method of claim 4, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

8. (Cancelled)

9. (Currently Amended): The method of ~~claim 8~~ claim 1, wherein the secure connection is a widget or window within a website provided by the merchant server.

10. (Currently Amended): The method of ~~claim 8~~ claim 1, wherein the secure connection is established via a static or dynamic uniform resource locator (URL).

11. (Currently Amended): The method of ~~claim 8~~ claim 1, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

12. (Currently Amended): The method of claim 1, wherein ~~the communications link used by the secure server to receive the financial account information provided by the payer~~ the secure connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data provided by the payer.

13. (Original): The method of claim 1, wherein the financial account information includes at least one of a credit card number or bank account number.

14. (Previously Presented): The method of claim 1, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

15. (Previously Presented): The method of claim 1, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

16. (Currently amended): A secure server that processes a payment from a payer to a payee, the secure server comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the secure computing system to:

receive an electronically-generated payment transaction instruction from a merchant server, the payment transaction instruction including at least one data element associated with the payer and specifying an amount of the payment from the payer to the payee;

establish ~~a communications link with the payer~~ a secure connection via the internet between the secure server and a computing system used by the payer to receive financial account information provided by the payer;

receive the financial account information provided by the payer via ~~the communications link~~ the secure connection;

provide an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the data token to the payer;

store the financial account information provided by the payer;

process the payment using the financial account information provided by the payer; and

forward at least a portion of the payment to the payee.

17. (Previously Presented): The secure server of claim 16, wherein the instructions further cause the secure computing system to:

receive a second payment transaction instruction from the merchant server, wherein the second payment transaction instruction includes a representation of the electronic data token and specifies an amount of a second payment from the payer to the payee;

process the second payment using the financial account information represented by the electronic data token; and

forward at least a portion of the second payment to the payee.

18. (Previously Presented): The secure server of claim 17, wherein the representation of the electronic data token is the electronic data token.

19. (Previously Presented): The secure server of claim 16, wherein the payment transaction instruction is generated by the merchant server using an application programming interface provided to the merchant server by the secure server.

20. (Previously Presented): The secure server of claim 19, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server.

21. (Previously Presented): The secure server of claim 19, wherein the application programming interface is implemented within a website hosted by the merchant server.

22. (Previously Presented): The secure server of claim 19, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer.

23. (Cancelled)

24. (Currently Amended): The secure server of ~~claim 23~~ claim 16, wherein the secure connection is a widget or window within a website provided by the merchant server.

25. (Currently Amended): The secure server of ~~claim 23~~ claim 16, wherein the secure connection is established via a static or dynamic uniform resource locator (URL).

26. (Currently Amended): The secure server of ~~claim 23~~ claim 16, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

27. (Currently Amended): The secure server of claim 16, wherein ~~the communications link used by the secure server to receive the financial account information provided by the payer~~ the secure connection is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

28. (Previously Presented): The secure server of claim 16, wherein the financial account information includes at least one of a credit card number or bank account number.

29. (Previously Presented): The secure server of claim 16, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

30. (Previously Presented): The secure server of claim 16, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

31. (Currently Amended): A method of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising:

receiving enrollment data identifying a payer;

generating an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of ~~a communications link between the secure server and the payer~~ a secure connection via the internet between the secure server and a computing system used by the payer for the secure server to receive financial account information provided by the payer;

outputting the electronic instruction to a communications network for transmittal to the secure server;

receiving, from the secure server, an electronic data token representing financial account information received by the secure server via ~~the communications link~~ the secure connection, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

storing the electronic data token in association with the enrollment data identifying the payer; and

processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token.

32. (Previously Presented): The method of claim 31, wherein the representation of the electronic data token is the electronic data token.

33. (Previously Presented): The method of claim 31, wherein the electronic instruction is generated using an application programming interface provided to the merchant server by the secure server.

34. (Previously Presented): The method of claim 33, wherein the application programming interface is implemented within a website hosted by the merchant server.

35. (Previously Presented): The method of claim 33, wherein the at least one data element associated with the payer is a customer identifier generated by the merchant server to identify the payer.

36. (Cancelled)

37. (Currently Amended): The method of ~~claim 36~~ claim 31, wherein the secure connection is a widget or window within a website provided by the merchant server.

38. (Currently Amended): The method of ~~claim 36~~ claim 31, wherein the secure connection provides access to the secure server using a static or dynamic universal resource locator (URL).

39. (Currently Amended): The method of ~~claim 36~~ claim 31, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

40. (Currently Amended): The method of claim 31, wherein the ~~communications link used to receive the financial account information provided by the payer~~ secure connection is

synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

41. (Previously Presented): The method of claim 31, wherein the enrollment data identifying the payer is received from the payer over a network.

42. (Previously Presented): The method of claim 31, wherein the financial account information includes at least one of a credit card number or bank account number.

43. (Previously Presented): The method of claim 31, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

44. (Previously Presented): The method of claim 31, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

45. (Previously Presented): The method of claim 31, wherein the payment processing system is the secure server.

46. (Currently Amended): A merchant server, operated by or for the benefit of a payee, comprising:

one or more computer processors; and

non-transitory computer readable storage media storing instructions that, when executed by the one or more computer processors, cause the merchant server to:

receive enrollment data identifying a payer;

generate an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of ~~a communications link between the secure server and the payer~~ a secure connection via the internet

between the secure server and a computing system used by the payer for the secure server to receive financial account information provided by the payer;

output the electronic instruction to a communications network for transmittal to the secure server;

receive, from the secure server, an electronic data token representing financial account information received by the secure server provided by the payer via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

store the electronic data token in association with the enrollment data identifying the payer; and

process a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token.

47. (New): The merchant server of claim 46, wherein secure connection is a widget or window within a website provided by the merchant server.

REMARKS

I. INTRODUCTION

The Office Action dated December 10, 2021 (hereinafter, "the pending Office Action") and the Interview Summary of February 17, 2022 (hereinafter, "the Interview Summary") have been carefully considered. In response thereto, the Applicant respectfully traverses the stated rejection. Accordingly, reconsideration and withdrawal of the outstanding Office Action and issuance of a Notice of Allowance are respectfully solicited in view of the following remarks.

II. STATUS OF THE CLAIMS

Claims 1-46 are pending. By way of this Amendment, independent claims 1, 16, 31, and 46 are amended to recite features previously recited in dependent claims 8, 23, and 36; dependent claims 9-12, 24-27, and 37-40 are amended for consistency with the independent claims; and new claim 47 is added to recite the features of dependent claim 37. No new matter is added.

III. SUMMARY OF THE OFFICE ACTION

In the pending Office Action, the pending claims are rejected under 35 U.S.C. § 101 as allegedly directed to non-patent eligible subject matter.

IV. INTERVIEW SUMMARY

At the outset, the Applicant would like to thank Examiner Pierre Maccagno and Supervising Patent Examiner Christine Behncke for the courtesies extended during the interview of February 11, 2022. During the interview, the Applicant argued that the pending Office Action does not clearly differentiate between the "abstract idea" identified by the Patent Office under Prong One of Step 2A (namely, processing a payment from a payer to a payee) and the "additional elements" that should be considered under Prong Two and Step 2B. Specifically, the Applicant argued that the stated rejection improperly characterizes the entire claim as an abstract idea[1] under Prong One of Step 2A and that the specific processing steps recited in the claims both "impose a meaningful limit" on the broad concept of processing a payment under Prong

[1] *See* Interview Agenda of February 10, 2022, Section B

Two of Step 2A[2] and amount to "significantly more" than a mere instruction to apply the broad concept of processing a payment on a computer under Step 2B.[3]

Examiner Behncke disagreed that the relevant standard under Prong Two is whether a claim "imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception" and, instead, appeared to believe that only claim elements directed to an improvement in technology are sufficient under Prong Two and Step 2B. Examiner Behncke also argued that the Federal Circuit holdings in *BASCOM*[4] and *Amdocs*[5] were not applicable because, in Examiner Behncke's opinion, the pending claims do not improve computer functionality. Additionally, Examiner Behncke argued that, under § 101, neither the manipulation of data nor adding additional nodes to a system are considered sufficient "additional elements." Furthermore, Examiner Behncke argued that the claimed processing steps were insufficient because "tokenization" was a known process. Finally, while not mentioned during the interview, the Interview Summary characterizes the processing steps recited in the claims as "insignificant extra solution activity."

V. PATENT ELIGIBLE SUBJECT MATTER REJECTION (35 U.S.C. § 101)

The Applicant respectfully disagrees with Examiner Behncke's interpretation of the subject matter eligibility guidelines. Improvements in the functioning of a computer (for example, as described in *Enfish*[6]) is only one way in which additional elements can integrate a judicial exception into a practical application. Meanwhile, the subject matter eligibility guidelines include a number of instances where the Federal Circuit has held that data processing steps[7] and/or adding additional nodes to a prior art system[8] – even an unconventional

[2] *See* Interview Agenda of February 10, 2022, Section C
[3] *See* Interview Agenda of February 10, 2022, Section C
[4] *BASCOM v. AT&T Mobility*, 827 F.3d 1341 (Fed. Cir. 2016)
[5] *Amdocs v. Openet Telecom*, 841 F.3d 1288 (Fed. Cir. 2016)
[6] *Enfish v. Microsoft*, 822 F.3d 1327 (Fed. Cir. 2016)
[7] See *BASCOM*, 827 F.3d at 1349 (filtering internet content using "any type of code which may be executed" along with database entries); *DDR Holdings, v. Hotels.com*, 773 F.3d 1245, 1257 (constructing and serving a hybrid web page that merges content associated with the products of the third-party merchant with stored "visually perceptible elements" from a host website)
[8] See *BASCOM*, 827 F.3d at 1343-44 (filtering internet content by the internet service provider server rather than on each local computer or a server located on a local network); *Amdocs v. Openet Telecom*, 841 F.3d at 1291-92 (performing known data gathering and filtering processes in a distributed architecture)

arrangement of well-known hardware components performing well-known processing steps[9] – integrated a judicial exception into a practical application under Prong Two of Step 2A and/or amounted to "significantly more" than a mere instruction to apply an abstract idea under Step 2B. As described below in Sections C through E, processing a payment by a server is a technical process akin to filtering internet content as described in *BASCOM* and/or displaying third-party advertisements on a host website as described in *DDR* and, similar to the ISP-level filtering arrangement described in *BASCOM* and the hybrid web page described in *DDR*, performing the processing steps recited in the claims by the secure server recited in the claims is a technical improvement to the prior art ways of processing payments over computer networks.

Even under Examiner Behncke's interpretation of the subject matter eligibility guidelines, however, the Applicant respectfully submits that the claims are patent eligible subject matter under § 101. As described in detail below in Section A, the claimed invention improves the functioning of the prior art merchant server itself by eliminating the need for that merchant server to include numerous computer components and to perform numerous computer processing steps required by the PCI Data Security Standard. Additionally, as described below in Section B, by moving the required computer components to a secure server that can provide functionality to multiple merchant servers, the claimed invention improves the functionality of the combined system (i.e., both the merchant servers and the secure server) by eliminating redundant computer components and redundant processing steps.

[9] In *BASCOM*, 827 F.3d at 1349, the claimed components ("local client computer," "remote ISP server," "Internet computer network," and "controlled access network accounts") were described in the specification as well known generic computer components. Meanwhile, the specification stated that "the filtering scheme can be any of a number of known-schemes, or hybrids thereof." *Id.* Similarly, in *Amdocs*, 841 F.3d at 1300-01, the court noted that the claims recited "arguably generic components," including network devices and "gathers" that gathered information. However, the court held that those generic components operated in an unconventional manner – working together in a distributed manner – to achieve an improvement in computer functionality.

A. The claimed invention improves the functioning of the prior art merchant server itself by eliminating the need for that merchant server to include numerous components and to perform numerous computer processing steps required by the PCI Data Security Standard

Claims that "purport to improve the functioning of the computer itself" are patent eligible under § 101.[10] In *Enfish*, for example, the Federal Circuit held that claims directed to a "self-referential" table were patent eligible because the self-referential table allowed for faster searching of data, allowed for more effective storage of data other than structured text, and allowed more flexibility in configuring the database.[11]

To process payments prior to the claimed invention, prior art merchant systems were required to receive, store, and transmit cardholder data. Therefore, as described in paragraphs [0004]-[0005] of the instant specification, prior art merchant systems were required to comply with Payment Card Industry (PCI) Data Security Standards. The PCI Data Security Standard that was in place on the effective filing date of the present application[12] is attached as Appendix A.

The claimed invention eliminates the need for merchant servers to receive, store, and transmit cardholder data by allowing those merchant servers to outsource the processing of cardholder data to the secure server. As a result, the claimed invention eliminates the need for that merchant server to comply with the PCI Data Security Standard of Appendix A. Instead, in the years since the claimed invention has become available, the Payment Card Industry Security Standards Council has published requirements applicable to "e-commerce merchants with a website(s) that does not itself receive cardholder data,"[13] which are attached as Appendix B. The PCI Data Security Standard of Appendix B is applicable to "e-commerce merchants who

[10] MPEP § 2106.05(a) citing *Alice v. CLS Bank*, 573 U.S. 208, 225 (2014); *see also* MPEP § 2106.04(d)(1) citing *Visual Memory v. NVIDIA*, 867 F.3d 1253, 1259-60 (Fed. Cir. 2017) (an enhanced computer memory system); *Finjan v. Blue Coat Systems*, 879 F.3d 1299 (Fed. Cir. 2018) (virus scanning); *SRI v. Cisco Systems*, 930 F.3d 1295, 1303 (Fed. Cir. 2019) (detecting suspicious activity by using network monitors and analyzing network packets)
[11] *Enfish v. Microsoft*, 822 F.3d 1327, 1333 (Fed. Cir. 2016)
[12] PCI DSS Requirements and Security Assessment Procedures, Version 2.0 (October 2010) (hereinafter, "PCI DSS v2.0")
[13] PCI Data Security Standard Self-Assessment Questionnaire (SAQ) A-EP and Attestation of Compliance; Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing, Version 3.2.1 (June 2018) (hereinafter, "PCI DSS v3.2.1 SAQ A-EP")

partially outsource their e-commerce payment channel to PCI DSS validated third parties," meaning "All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor."[14]

As described below, the PCI Data Security Standard of Appendix B does not require that merchant systems that outsource the processing of cardholder data to the secure server recited in the claims include a number of computer components or perform a number a computer processing steps that were required of prior art merchant systems that received cardholder data. Additionally, if any of the requirements of the PCI Data Security Standard of Appendix B are not applicable, that PCI Data Security Standard allows those merchants to simply indicate that those requirements are not applicable.[15] Meanwhile, as described below, several requirements of the PCI Data Security Standard of Appendix B are not applicable to merchant systems that outsource the processing of cardholder data to the secure server recited in the claims. Therefore, just like the self-referential table at issue in *Enfish* improved the functioning of the computer itself, the claimed invention improves the functioning of the merchant server itself by eliminating the need for that merchant server to include the following components and to perform the following computer processing.

Prior to the claimed invention, prior art merchant systems were required to protect stored cardholder data by rendering any primary account number (PAN) unreadable anywhere it is stored[16] by one-way hashing the entire PAN using strong cryptography, using index tokens and securely stored pads, or using strong cryptography with associated key-management processes and procedures.[17]

Prior art merchant systems were required to generate strong data-encrypting cryptographic keys,[18] encrypt those data-encrypting cryptographic keys using key-encrypting

[14] Page iii
[15] *See* PCI DSS v3.2.1 SAQ A-EP, Appendix C: Explanation of Non-Applicability
[16] including on portable digital media, backup media, and in logs
[17] Requirement 3.4. If the "full PAN is not needed" (page 28), the PCI Data Security Standard also permitted truncation of cardholder data as long as truncated segment of the PAN was not hashed. However, to process a payment, prior art merchant systems needed to store the full PAN.
[18] Requirement 3.6.1

cryptographic keys,[19] store the key-encrypting cryptographic keys separately from the data-encrypting cryptographic keys,[20] and securely distribute the data-encrypting cryptographic keys.[21] Prior art merchant systems were required to change cryptographic keys that had reached the end of their cryptoperiod (e.g., after a defined period of time and/or a defined amount of ciphertext had been produced).[22] Prior art merchant systems were also required to include functionality to retire or replace cryptographic keys when required,[23] for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key).[24] Prior art merchant systems were also required to mask PAN when displayed.[25]

If the prior art merchant system used disk encryption,[26] the prior art merchant system was required to manage logical access independently of native operating system access control mechanisms.[27] A prior art merchant system was not compliant with the PCI Data Security Standard if it used local user account databases or tied decryption keys to user accounts.[28]

If the prior art merchant system used manual clear-text cryptographic key management operations, the prior art merchant system was required to provide functionality to manage those operations using split knowledge and dual control.[29] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key.[30]

To avoid the requirement to conduct quarterly manual reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy,

---

[19] Requirements 3.5.2, Testing Procedure 3.5.2.a
[20] *Ibid.*
[21] Requirement 3.6.2
[22] Requirement 3.6.4
[23] The retirement or replacement of a cryptographic key was required if the cryptographic key was suspected of being compromised or when the integrity of the cryptographic key had been weakened (for example, if an employee with knowledge of a clear-text cryptographic key left the organization)
[24] Requirement 3.6.5
[25] Requirement 3.3
[26] rather than file- or column-level database encryption
[27] Requirement 3.4.1
[28] *Ibid.*
[29] Requirement 3.6.6
[30] *Ibid.*

a prior art merchant system was required to include a programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy.[31]

Except in limited circumstances,[32] prior art merchant systems were required to perform a process to securely delete sensitive authentication data received from cardholders, including the full contents of any magnetic stripe or chip,[33] any card validation code,[34] and any personal identification number (PIN) or encrypted PIN block.[35] While merchant systems that partially outsource their e-commerce payment channel using the claimed invention are still required to securely delete any sensitive authentication data they receive,[36] the claimed invention allows merchant systems to process payments without receiving any sensitive authentication data.

Prior art merchant systems were required to use strong cryptography and security protocols to safeguard sensitive cardholder data transmitted over open, public networks such as the Internet, wireless networks, and mobile networks.[37] The PCI Data Security Standard suggested using SSL/TLS, IPSEC, or SSH to transmit sensitive cardholder data over open, public networks.[38] Prior art merchant systems were required to accept only trusted cryptographic keys and/or certificates,[39] to use a protocol implemented to use only secure configurations (that did not support insecure versions or configurations),[40] and to use "the proper encryption strength" (according to vendor recommendations/best practices) for the encryption methodology in use.[41] Prior art merchant systems were required to render PAN unreadable or secured with strong cryptography whenever sent to end-user messaging technologies such as email, instant

[31] Requirement 3.1.1, Testing Procedure 3.1.1.d
[32] Issuers and companies that support issuing services were permitted to securely store sensitive authentication data if there was "a business justification" to store that sensitive authentication data
[33] Requirement 3.2.1
[34] Requirement 3.2.2
[35] Requirement 3.2.3
[36] PCI DSS v3.2.1 SAQ A-EP, Requirement 3
[37] PCI DSS v2.0, Requirement 4.1
[38] *Ibid.*
[39] Requirement 4.1, Testing Procedure 4.1.b
[40] Requirement 4.1, Testing Procedure 4.1.c
[41] Requirement 4.1, Testing Procedure 4.1.d

messaging, or chat programs.[42] Again, merchants who partially outsource their e-commerce payment channel using the claimed invention are still required to safeguard any sensitive cardholder data they transmit.[43] However, the claimed invention allows merchant systems to process payments without transmitting any sensitive cardholder data.

Wireless networks transmitting cardholder data or connected to the cardholder data environment were required to use industry best practices to implement strong encryption for authentication or transmission.[44] The PCI Data Security Standard noted that the use of Wired Equivalent Privacy (WEP) as a security control was prohibited and suggested IEEE 802.11i as an example of industry best practices.[45] Note that the IEEE 802.11i standard makes use of the Advanced Encryption Standard (AES) block cipher, which requires a dedicated chip that was not commonly included in most wireless network hardware.[46]

B. Additionally, because the secure server recited in the claims can perform cardholder data functions for multiple merchant servers, the claimed invention improves the functioning of the combined system for processing payments (i.e., both the merchant servers and the secure server) by eliminating redundant computer components and redundant processing steps

The claimed invention allows multiple merchant systems to outsource the processing of cardholder data to the secure server recited in the claims while maintaining PCI compliance as described in the PCI Data Security Standard of Appendix B. Accordingly, rather than *each* merchant system being required to include the required computer components, only the secure server is required to include many of the computer components required by the PCI Data Security Standard of Appendix A. Additionally, rather than *each* merchant system being required to perform each of the software processing steps required by the PCI Data Security Standard of Appendix A, many of those software processing steps are only required to be

[42] Requirement 4.2, Testing Procedure 4.2.a
[43] PCI DSS v3.2.1 SAQ A-EP, Requirement 4
[44] PCI DSS v2.0, Requirement 4.1.1
[45] *Ibid.*
[46] See 802.11i, TechTarget, June 2006, https://www.techtarget.com/searchmobilecomputing/definition/80211i

performed once by the secure server recited in the claims for each of those merchant systems to maintain PCI compliance.

When providing functionality for payers of multiple merchants to provide PAN (e.g., via an application programming interface (API)[47] or a secure connection via the internet,[48] such as a redirect URL[49] or a widget or window within a website provided by the merchant server[50]), the secure server can provide a single interface that masks that PAN when displayed,[51] a single process to remove stored cardholder data exceeding the requirements defined in the secure system's data retention policy,[52] and a single process to securely delete sensitive authentication data.[53]

The secure system can protect that cardholder data for all of those merchant systems by generating strong data-encrypting cryptographic keys, encrypting those data-encrypting cryptographic keys using key-encrypting cryptographic keys, securely storing the cryptographic keys, and retiring or replacing the cryptographic keys when required.[54] One particularly beneficial improvement provided by the claimed invention is the secure system can perform a single key rotation process and ensure that all cryptographic keys used for all merchants are changed before they reach the end of their cryptoperiod.[55]

While receiving and transmitting sensitive cardholder data for multiple merchants, the secure server recited in the claims only requires one set of components that uses strong cryptography and security protocols to safeguard that sensitive cardholder data during transmission over open, public networks[56] (including wireless network hardware with the

[47] e.g., via an application programming interface (API) as recited in dependent claims 4-7, 19-22, and 33-35,
[48] Dependent claims 8-11, 23-26, and 35-39
[49] Dependent claims 11, 26, and 39
[50] Dependent claims 9, 24, and 37
[51] PCI DSS v2.0, Requirement 3.3
[52] Requirement 3.1.1, Testing Procedure 3.1.1.d
[53] Requirement 3.2
[54] Requirement 3.4 through Requirement 3.6
[55] Requirement 3.6.4
[56] Requirement 4.1

dedicated chip[57] required by the IEEE 802.11i standard[58] if needed to transmit cardholder data wirelessly).

C. Processing a payment, by a server, is a technical process

In addition to improvements to computer functionality, the subject matter eligibility guidelines recognize that "an improvement to other technology or technical field" may integrate a judicial exception into a practical application under Prong Two of Step 2A or recite "significantly more" than an instruction to apply the judicial exception under Step 2B. In *BASCOM*, the claims were directed to filtering content on the internet.[59] As described in *BASCOM*, prior art content filtering methods included installing filtering software on each local computer.[60] However, it was "difficult and time consuming to install" that software "on every end-user's client machine."[61] Other prior art methods included relocating the filtering software to a local server or an ISP.[62] However, those "one-size-fits-all" solutions were not ideal because "a single set of filtering criteria is often not appropriate for all of the end-users."[63] Therefore, the claims at issue in *BASCOM* provided individually customizable filtering at the remote ISP server.[64] The ISP stored customized filtering mechanisms for different users, required each user to log in, and applied the filtering mechanisms associated with each user.[65] The Federal Circuit noted that, when viewed individually, the claimed components ("local client computer," "remote ISP server," "Internet computer network," and "controlled access network accounts") were described in the specification as well-known, generic computer components.[66] Meanwhile, the specification stated that "the filtering scheme" performed by those components "can be any of a number of known-schemes, or hybrids thereof."[67] However, the Federal Circuit held that the claims were patent eligible under § 101 because the "particular arrangement of elements" was "a

[57] *See* 802.11i, TechTarget, June 2006, https://www.techtarget.com/searchmobilecomputing/definition/80211i
[58] PCI DSS v2.0, Requirement 4.1.1
[59] 827 F.3d at 1341
[60] *Id.* at 1333
[61] *Id.* at 1344
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.* at 1345-46
[66] *Id.* at 1349
[67] *Id.* at 1350

technical improvement over prior art ways of filtering such content." Installing a filtering tool at a location remote from the end-users, with customizable filtering features specific to each end user, gave that filtering tool both the benefits of a filter on a local computer and the benefits of a filter on the ISP server.[68] The court also noted that the claims do not "preempt all ways of filtering content on the Internet" but "rather, they recite a specific, discrete implementation of the abstract idea of filtering content."[69]

In *DDR Holdings*, the claims were directed to constructing and serving a hybrid web page that merges content associated with the products of the third-party merchant with stored "visually perceptible elements" from a host website.[70] There, the specific issue was that, "upon the click of an advertisement for a third-party product displayed on a host's website, the host website would lose that visitor as he or she is "transported to the third party's website."[71] To solve that problem, the claims were directed to "an automatically-generated hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website related to the clicked advertisement" so that, "rather than instantly losing visitors to the third-party's website, the host website can instead send its visitors to a web page on the outsource provider's server that 1) incorporates 'look and feel' elements from the host website, and 2) provides visitors with the opportunity to purchase products from the third-party merchant without actually entering that merchant's website."[72] The Federal Circuit held that such claims were patent eligible "because they do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet" and instead provided a claimed solution that was "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks."[73] The court also noted that the claims "do not attempt to preempt every application of the idea of increasing sales by making two web pages look the same," but rather "recite a specific way to automate the creation of a composite web page by an 'outsource provider' that

[68] *Id.*
[69] *Id.*
[70] 773 F.3d at 1257
[71] *Id.*
[72] *Id.* at 1257-1258 (internal footnote omitted)
[73] *DDR*, 773 F.3d at 1257

incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet."[74]

In both instances, the Federal Circuit held that the claims improved a technical process. As explained by the court in *BASCOM*:

> Although the invention in DDR's patent was engineered in the context of retaining potential customers, the invention was not claiming a business method *per se*, but was instead claiming a technical way to satisfy an existing problem for website hosts and viewers. Similarly, although the invention in the '606 patent [at issue in *BASCOM*] is engineered in the context of filtering content, the invention is not claiming the idea of filtering content simply applied to the Internet. The '606 patent is instead claiming a technology-based solution (not an abstract-idea-based solution implemented with generic technical components in a conventional way) to filter content on the Internet that overcomes existing problems with other Internet filtering systems. By taking a prior art filter solution (one-size-fits-all filter at the ISP server) and making it more dynamic and efficient (providing individualized filtering at the ISP server), the claimed invention represents a software-based invention that improves the performance of the computer system itself.[75]

Similarly, the claims at issue are directed to the technical process of processing a payment using a server. While the invention is used in service of a business transaction, the claims are not directed to the process of marketing or arranging that business transaction, but rather to the technical process of receiving, safeguarding, and transmitting cardholder data while complying with the PCI Data Security Standard. As described in the instant specification (e.g., with reference to FIGS. 4a through 4l), receiving and transmitting cardholder data is a technical process. Meanwhile, as described in exhausting detail in Sections A and B above, complying with the PCI Data Security Standard to safeguard that cardholder data requires specific computer components and the performance of specific computer processing steps.

[74] *Id.* at 1259
[75] *BASCOM*, 827 F.3d at 1351 (internal citation omitted)

D. The claimed invention improves the prior art process of processing a payment by eliminating the need for merchants to integrate their systems with the components required for PCI compliance

Prior to the claimed invention, merchants were required to integrate their systems with the computer components required for PCI compliance described in Sections A and B above, while ensuring that those components did not negatively impact the functions performed by the merchant system, including the user experience provided to their customers. By enabling those merchants to outsource the processing of cardholder data to the secure server recited in the claims, the secure server and merchant server recited in the claims form a hybrid system (similar to the hybrid webpage[76] at issue in *DDR*[77]) that enables merchants to focus their efforts on their own core systems – and the user experience provided to their customers – while maintaining compliance with the PCI Data Security Standard of Appendix B.

E. Additionally, the claimed invention improves the prior art process of processing a payment by eliminating the need for each merchant to perform numerous tasks to comply with the PCI Data Security Standard

As described above, the Federal Circuit in *BASCOM* held that filtering content at the ISP server (rather than on each end-user's client machine) was patent eligible under § 101 because it eliminated the "difficult and time consuming" process of installing software "on every end-user's client machine."[78]

In addition to the required computer components and computer processing steps outlined in Sections A and B above, the PCI Data Security Standard also required that employees or agents of merchants using prior art merchant systems perform all of the tasks outlined in detail below. By providing functionality for multiple merchants to outsource the processing of

[76] Note that, in embodiments of dependent claims 9, 24, 37, and 47, where the secure connection via the internet between the secure server and the computing system used by the payer "is a widget or window within a website provided by the merchant server," the claimed solution is strikingly similar to the solution in *DDR* in that it is "an automatically-generated hybrid web page that combines visual 'look and feel' elements" from the merchant server website and functionality to provide financial account information to the third-party secure server. In those embodiments, the merchant server sends its visitors to a website "that 1) incorporates 'look and feel' elements from the [merchant server] website, and 2) provides visitors with the opportunity" to submit sensitive financial account information to the third-party secure server "without actually entering" that secure server's website.
[77] *DDR*, 773 F.3d at 1257-58
[78] *BASCOM*, 827 F.3d at 1344

cardholder data, the claimed invention improves the prior art process of processing a payment by eliminating the need for each merchant to individually perform those tasks. Therefore, just like BASCOM's process of filtering internet content by an ISP server (rather than on each end-user's client machine) improved the prior art internet content filtering processes, outsourcing the receipt, storage, and processing of cardholder data from each merchant's system to the secure server recited in the claims improved the prior art payment processing process by eliminating the need for each merchant to each perform all of those tasks.

Prior to the claimed invention, merchants using prior art merchant systems were required to verify that the prior art merchant systems complied with each and every one of the requirements above.

To protect stored cardholder data, merchants were required to implement data retention and disposal policies, procedures, and processes to keep cardholder data storage to a minimum.[79] To comply with the PCI Data Security Standard, the data retention and disposal policy was required to limit data storage and retention time "to that which is required for legal, regulatory, and business requirements."[80] Merchants were required to have specific retention requirements for all cardholder data[81] specifying the time period that cardholder data needed to be stored and the legal, regulatory, or business reason why that cardholder data needed to be stored for that time period.[82] The data retention and disposal policy was also required to include provisions for secure disposal of data (including disposal of cardholder data) when no longer needed for those legal, regulatory, or business reasons.[83] If the merchant system did not include the programmatic process to automatically remove stored cardholder data exceeding the requirements defined in the merchant's data retention policy, the merchant was required to conduct quarterly reviews to verify that stored cardholder data did not exceed the requirements defined in the merchant's data retention policy.[84]

---

[79] Requirement 3.1
[80] Requirement 3.1.1
[81] Requirement 3.1.1, Testing Procedure 3.1.1.c
[82] Requirement 3.1.1, Testing Procedure 3.1.1.a
[83] Requirement 3.1.1, Testing Procedure 3.1.1.b
[84] Requirement 3.1.1, Testing Procedure 3.1.1.d

Merchants were required to examine data sources – including incoming transaction data, all logs (e.g., transaction logs, history logs, debugging logs, and error logs), history files, trace files, several database schemas, and database contents – to verify that the full contents of magnetic stripes or chips,[85] card validation codes,[86] and PINs or encrypted PIN blocks[87] were not stored under any circumstance.

To verify that displayed PAN was masked, merchants were required to obtain and examine writing policies and examine displays of PAN (e.g., on screen or on paper receipts) to verify that the PAN was masked[88] and examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[89]

To verify that stored PAN was rendered unreadable, merchants were required to examine documentation about the system, including the vendor, the type of system/process, and any applicable encryption algorithms.[90] Additionally, merchants were required to confirm that PAN was rendered unreadable by examining several tables or files from a sample of data repositories,[91] a sample of removable media (e.g., back-up tapes),[92] and a sample of audit logs.[93]

To protect cryptographic keys, merchants were required to document and implement key-management processes and procedures.[94] The key-management processes and procedures were required to restrict access to the fewest number of custodians necessary[95] and to store cryptographic keys in the fewest possible locations and forms.[96] Merchants were required to periodically change cryptographic keys once they reached the end of their cryptoperiod (for example, as after a defined period of time had passed and/or after a defined amount of cipher-text had been produced) as defined by the associated application vendor or key owner and based

[85] Requirement, 3.2.1, Testing Procedure 3.2.1
[86] Requirement, 3.2.2, Testing Procedure 3.2.2
[87] Requirement, 3.2.3, Testing Procedure 3.2.3
[88] Requirement 3.3, Testing Procedure 3.3
[89] Requirement, 3.4, Testing Procedure 3.4.a
[90] Requirement, 3.4, Testing Procedure 3.4.a
[91] Requirement, 3.4, Testing Procedure 3.4.a
[92] Requirement, 3.4, Testing Procedure 3.4.c
[93] Requirement, 3.4, Testing Procedure 3.4.d
[94] Requirement 3.6
[95] Requirement 3.5.1
[96] Requirement 3.5.2, Testing Procedure 3.5.2.b

on industry best practices and guidelines (e.g., NIST Special Publication 800-57).[97] Merchants were also required to retire or replace cryptographic keys if the cryptographic key was suspected of being compromised[98] or when the integrity of the cryptographic key had been weakened (for example, if an employee with knowledge of a clear-text cryptographic key left the organization),[99] for example by destroying and/or revoking cryptographic keys and, if necessary, securely archiving those retired or replaced cryptographic keys (e.g., using a key encryption key).[100]

If the merchant system used manual clear-text cryptographic key management operations, the merchant was required to manage those operations using split knowledge and dual control.[101] For example, the PCI Data Security Standard suggested a system requiring two or three people, each knowing only their own key component, to reconstruct the whole key.[102] The merchant key-management procedures were required to prevent unauthorize substitution of cryptographic keys.[103] Merchants were required to obtain written or electronic acknowledgement from all custodians of the cryptographic keys that those custodians understood and accepted their key-custodian responsibilities.[104]

Merchants were required to observe a sample of transactions as they occurred to verify that cardholder data was encrypted during transit.[105] For SSL/TLS implementations, merchants were required to verify that HTTPS appeared as a part of the browser Universal Record Locator (URL) and that no cardholder data was required when HTTPS does not appear in the URL.[106] Merchants were also required to maintain a policy stating that unprotected PANs were not to be sent via end-user messaging technologies.[107]

---

[97] Requirement 3.6.4
[98] Requirement 3.6.5, Testing Procedure 3.6.5.b
[99] Requirement 3.6.5, Testing Procedure 3.6.5.a
[100] Requirement 3.6.5
[101] Requirement 3.6.6
[102] *Ibid.*
[103] Requirement 3.5.7, Testing Procedure 3.6.7
[104] Requirement 3.5.8, Testing Procedure 3.6.8
[105] Requirement 4.1, Testing Procedure 4.1.a
[106] Requirement 4.1, Testing Procedure 4.1.e
[107] Requirement 4.2, Testing Procedure 4.2.b

F. The specific processing steps recited in the claims are not "extra-solution activity" and the Patent Office provides no evidence that those processing steps were so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement of 35 U.S.C. § 112(a)

To support a factual determination that claimed features were "well-understood, routine, conventional activity," the subject matter eligibility guidelines require factual evidence that the specific "combination"[108] of elements recited in the claims were so "widely prevalent or in common use in the relevant industry" that they "need not be described in detail in the patent specification" to satisfy the written description requirement of 35 U.S.C. § 112(a).[109] The pending Office Action provides no evidence that the specific processing steps recited in the claims performed by the secure server recited in the claims are known, let alone so "widely prevalent" that they did not need description in a patent specification.

The Interview Summary states that "the additional insignificant extra solution activity amount only to data gathering and data storing that are recognized by courts as well-understood routine conventional." First, the term "extra-solution activity" refers to "activities incidental to the primary process or product that are merely a nominal or tangential addition to the claim."[110] Here, the claimed processing steps are not "incidental to the primary process" or "merely a nominal or tangential addition to the claim." Instead, performing those processing steps by the secure server (thereby outsourcing the processing of cardholder data) differentiates the claimed invention from a conventional transaction where a payer provides financial account information directly to the merchant server.

Second, courts have not held that performing the specific "combination" of features recited in the claims – a secure server receiving an electronically-generated payment transaction instruction from a merchant server, establishing a secure connection via the internet with a computing system used by the payer to receive financial account information provided by the payer, receiving the financial account information provided by the payer via the secure connection, providing an electronic data token (representing the financial account information

[108] MPEP § 2106.05(e) citing *BASCOM*, 827 F.3d at 1349
[109] MPEP § 2106.05(d)(I)(1)
[110] MPEP § 2106.05(g)

provided by the payer) to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer, storing the financial account information provided by the payer, and processing the payment using the financial account information provided by the payer – are well-understood, routine or conventional.

Accordingly, the Applicant respectfully submits that the pending claims are patent eligible subject matter under § 101.

VI. CONCLUSION

In view of the above Remarks, the Applicant believes the pending application is in condition for allowance.

Please charge any shortage or credit any overpayment of fees to BLANK ROME LLP, Deposit Account No. 23-2185, under Order No. 124452.00122. In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition does not accompany this Amendment or is insufficient to render this Amendment timely, the Applicant hereby petitions under 37 C.F.R. §1.136(a) for an extension of time for as many months as required to render this submission timely. Any fee due is authorized above.

Dated: April 11, 2022

Respectfully submitted,

By: /Michael C. Greenbaum/
Michael C. Greenbaum
Registration No.: 28,419
BLANK ROME LLP
Correspondence Customer Number: 27557
Attorney for Applicant

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

27557 7590 02/17/2022

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER	
MACCAGNO, PIERRE L	
ART UNIT	**PAPER NUMBER**
3697	
NOTIFICATION DATE	**DELIVERY MODE**
02/17/2022	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

WashingtonDocketing@blankrome.com
jyeddo@BlankRome.com

Applicant-Initiated Interview Summary	Application No. 16/535,424	Applicant(s) POLLIN et al.		
	Examiner PIERRE L MACCAGNO	Art Unit 3697	AIA (First Inventor to File) Status No	Page 1 of 2

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
PIERRE L MACCAGNO	Examiner	Telephonic
CHRISTINE BEHNCKE	SPE	
JONATHAN KING (Reg #65967)	Attorney	

Date of Interview: 11 February 2022

Issues Discussed:

35 U.S.C. 101

The Applicant provided an agenda attached to this interview summary.

The Applicant set up an interview in order to understand the reasoning behind the 101 rejection.

The Applicant argued that under step 2A Prong One the use of a secure server to process a payment from a payer to a merchant – by establishing a communications link with a payer to receive financial account information and providing an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer) – so that the merchant server can process a transaction without having access to (or being required to secure) the underlying financial account information is not “a fundamental economic practice” under § 101 and hence is not an abstract idea.

Furthermore the Applicant argued that even if the claims are broadly characterized as describing one method of processing a payment from a payer to a payee, the specific processing steps above “impose a meaningful limit” on that broad concept such that the claims are directed to a specific, “practical application” of that broad concept.

Finally the Applicant argued that the specific technical features recited in the claims also amount to “ significantly more” than “a mere instruction to apply” the abstract idea of processing a payment from a payer to a payee “on a computer and hence represent an "inventive concept".

The Examiner disagreed that there are additional elements in the claim that impose a meaningful limit on the abstract idea or that they provide an inventive concept since the additional elements recite standard computer components used as a tool to implement the abstract idea, and there is nothing in the claims or specification that would indicate an improvement in technology. Furthermore the additional insignificant extra solution activity amount only to data gathering and data storing that are recognized by the courts as well-understood routine conventional..

The Applicant's agenda is included as part of this communication as required by USPTO interview policy .

No agreements were reached.

Applicant-Initiated Interview Summary	**Application No.** 16/535,424	**Applicant(s)** POLLIN et al.		
	Examiner PIERRE L MACCAGNO	**Art Unit** 3697	**AIA (First Inventor to File) Status** No	**Page** **2 of 2**

☑ Attachment

/PIERRE L MACCAGNO/ Examiner, Art Unit 3697	/CHRISTINE M BEHNCKE/ Supervisory Patent Examiner, Art Unit 3697

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Docket No.: 124452.00122
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert Evan POLLIN et al.

Application No.: 16/535,424 | Confirmation No.: 2047

Filed: August 8, 2019 | Art Unit: 3696

For: ENROLLING A PAYER BY A MERCHANT SERVER OPERATED BY OR FOR THE BENEFIT OF A PAYEE AND PROCESSING A PAYMENT FROM THE PAYER BY A SECURE SERVER | Examiner: Pierre L. MACCAGNO

INTERVIEW AGENDA

Pierre Maccagno
Christine M. Behncke
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiners Maccagno and Behncke:

In anticipation of our interview tomorrow at 1 pm ET, please consider the following Interview Agenda, which is not intended to be made of record.

Dated: February 10, 2022

Respectfully submitted,

By: /Jonathan R. King/
Jonathan R. King
Registration No.: 65,967
BLANK ROME LLP
Correspondence Customer Number: 27557
Attorney for Applicant

A. Claimed Features

Merchants spend considerable time, effort, and expense securing the financial information (e.g., credit card numbers, bank account numbers) received from purchasers in order to provide a secure platform for purchasers and comply with industry security standards. The claimed invention eliminates that burden by allowing the merchant (payee) and the purchaser (payer) to conduct a transaction without the merchant receiving – and thus having to safeguard – the financial information of the purchaser.

> 1. A method[1] of processing a payment from a payer to a payee, the method being performed by a secure server [e.g., 202], the method comprising:
> receiving an electronically-generated payment transaction instruction from a merchant server [e.g., 204], the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee;
> establishing a communications link with the payer to receive financial account information provided by the payer;
> receiving the financial account information provided by the payer via the communications link;
> providing an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;
> storing the financial account information provided by the payer;
> processing the payment using the financial account information provided by the payer; and
> forwarding at least a portion of the payment to the payee.
>
> ...
>
> 31. A method[2] of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising:
> receiving enrollment data identifying a payer;
> generating an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a communications link between the secure server and the payer for the secure server to receive financial account information provided by the payer;
> outputting the electronic instruction to a communications network for transmittal to the secure server;

[1] Independent claim 16, which is directed to the secure server, recites analogous features.
[2] Independent claim 46, which is directed to the merchant server, recites analogous features.

receiving, from the secure server, an electronic data token representing financial account information received by the secure server via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

storing the electronic data token in association with the enrollment data identifying the payer; and

processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token.

The claims recite a secure server [e.g., 202] in communication with a merchant server [e.g., 204]. In response to an electronically-generated payment transaction instruction from the merchant server, the secure server establishes a communications link with the payer to securely receive sensitive financial account information provided by the payer. An electronic data token representing the payer's financial account information is generated. The secure server provides that electronic data token to the merchant server. Critically, the secure server provides the electronic data token without providing the underlying financial account information to the merchant server (or providing the electronic data token to the payer). The secure server and the electronic data token enable payments from a payer to payee to the processed without the payee having to receive, store, and safeguard the underlying financial account information.

In some embodiments, the secure server may provide an application programming interface (API),[3] in some instances implemented within a website hosted by the merchant server,[4] with functionality for the merchant server to transmit the payment transaction instruction. The communications link between the payer and the secure server may be a secure connection via the internet,[5] such as a redirect URL.[6] The secure connection may be a widget or window within a website provided by the merchant server,[7] so that the process of interacting

[3] Dependent claims 4-7, 19-22, and 33-35
[4] Dependent claims 6, 21, and 34
[5] Dependent claims 8-11, 23-26, and 35-39
[6] Dependent claims 11, 26, and 39
[7] Dependent claims 9, 24, and 37

with the merchant server while transmitting sensitive financial account information to the secure server is seamless from the viewpoint of the customer.[8]

Because the electronic data token is non-sensitive, the merchant server may store the electronic data token (without having to comply with stringent compliance requirements) and, in some embodiments, that electronic data token may be used to process future payments authorized by the payer.

B. Step 2A, Prong One: The specific processing steps recited in the claims are not one of "the basic tools of scientific and technological work" excluded from patentability under § 101 because "monopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it"

"There is no dispute ... that many computer-implemented claims are formally addressed to patent-eligible subject matter."[9] Computer-implemented business methods are also patent eligible. "[A] business method is simply one kind of 'method' that is, at least in some circumstances, eligible for patenting under § 101."[10] Inventions in one of the four broad statutory categories[11] are patent eligible unless they are directed to one of "the basic tools of scientific and technological work" – namely, "laws of nature, natural phenomena, and abstract ideas" – where "monopolization of those tools through the grant of a patent" might "inhibit further discovery by improperly tying up the future use of these building blocks of human ingenuity."[12]

Courts have identified "abstract ideas" under § 101 only by way of example. Examples of concepts that courts have found patent ineligible include claims that would preempt "fundamental economic principles or practices", such as intermediated settlement,[13] hedging risk,[14] rules for conducting a wagering game,[15] offer-based price optimization,[16] using a marking

[8] See paragraph [0046] of the specification
[9] *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*, 134 S. Ct. 2347, 2358-59 (2014)
[10] *Bilski v. Kappos*, 130 S.Ct. 3218, 3228 (2010)
[11] process, machine, manufacture, or composition of matter
[12] *Alice*, 134 S.Ct. at 2354 citing *Mayo Collaborative v. Prometheus Labs*, 132 S.Ct. 1289, 1293 (2012)
[13] *Id.*
[14] *Bilski*, supra
[15] *In re Smith*, 815 F.3d 816, 818-19, (Fed. Cir. 2016)
[16] *OIP Techs. v. Amazon.com*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015)

affixed to the outside of a mail object to communicate information about the mail object,[17] placing an order based on displayed market information,[18] and a retailer allowing a customer requesting goods remotely (e.g., via the internet or by phone) to pay in person at a retail location.[19]

The pending Office Action argues that all of the following processing steps are directed to the fundamental economic practice of "processing a payment from a payer to a payee": receiving an electronically-generated payment transaction instruction from a merchant server that includes a data element associated with a payer and specifies an amount of a payment from the payer to a payee; establishing a communications link with the payer to receive financial account information provided by the payer; providing an electronic data token (representing financial account information provided by the payer) to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer; processing the payment using the financial account information provided by the payer; and forwarding at least a portion of the payment to the payee.[20]

However, the Applicant respectfully submits that using a secure server to process a payment from a payer to a merchant – by establishing a communications link with a payer to receive financial account information and providing an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer) – so that the merchant server can process a transaction without having access to (or being required to secure) the underlying financial account information is not "a fundamental economic practice" under § 101.

---

[17] *Inventor Holdings v. Bed Bath Beyond*, 876 F.3d 1372, 1378-79 (Fed. Cir. 2017)
[18] *Trading Technologies Int'l v. IBG*, 921 F.3d 1084, 1092 (Fed. Cir. 2019)
[19] *Inventor Holdings v. Bed Bath & Beyond*, 123 F. Supp. 3d 557, 561 (D. Del. 2015) *aff'd* 643 Fed.Appx. 1014, 1015 (Fed. Cir. 2016)
[20] The pending Office Action states that "Applicant does not argue against the claims being directed to an abstract idea" in the Response of September 9, 2021. This is not true. As is repeated here, Applicant argued that the specific technical features recited in the claims are "not 'a fundamental economic practice'" under Step 2A, Prong One and, "[e]ven if the claims are not a broadly characterized as *describing* one method of processing a payment from a payer to a payee (Step 2A Prong One)," the claims are not "directed to" that fundamental economic practice under Step 2A Prong Two because "the claims can hardly be characterized as 'a drafting effort designed to monopolize' the broad concept of processing a payment from a payer to a payee" (emphasis original).

C. Step 2A, Prong Two: Even if the claims are broadly characterized as *describing* one method of processing a payment from a payer to a payee, the specific processing steps above "impose a meaningful limit" on that broad concept such that the claims are directed a specific, "practical application" of that broad concept

The Supreme Court "has long distinguished between principles themselves (which are not patent eligible) and the integration of those principles into practical applications (which are patent eligible)."[21] Accordingly, even if a claim *recites* a judicial exception (Step 2A Prong One), MPEP § 2106.04(d) instructs examiners to "evaluate whether the claim as a whole integrates the recited judicial exception into a practical application of the exception." (Step 2A Prong Two). "A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception."[22] For instance, "the claimed invention may integrate the judicial exception into a practical application by demonstrating that it improves the relevant existing technology."[23]

Even if the claims are broadly characterized as *describing* one method of processing a payment from a payer to a payee (Step 2A Prong One), the claims can hardly be characterized as "a drafting effort designed to monopolize" the broad concept of processing a payment from a payer to a payee (Step 2A Prong Two).[24] Instead, the claims "impose a meaningful limit" on the broad concept of *processing a payment* by further reciting specific technical features – namely, a secure server that, in response to an electronically-generated payment transaction instruction from a merchant server (including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee), establishes a communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without

[21] MPEP 2106.04(d) citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 80, 84 (2012)
[22] *Id.*
[23] MPEP 2106.04(d)(1). Note that, in Step 2A Prong One, whether the claim "pertains to" technological improvement is determined "without reference to what is well-understood, routine, conventional activity."
[24] Note that, if the claims *were* a drafting effort designed to monopolize the concept of processing payments, it would be quite a poor effort. One could simply and easily design around this attempted monopoly by not employing a secure server that performs the claimed processing steps. Instead, a merchant server could simply be configured to receive the financial account information directly from the payer and process the payment.

providing the electronic data token to the payer). Those specific technical features direct the claim to a specific, practical application of that broad concept – namely, processing a transaction from a payer to a payee without the payee having access to (or being required to secure) the underlying financial account information.

In the MPEP, the most relevant example of a "fundamental economic principle or practice" is the system directed to "local processing of payments for remotely purchased goods" at issue in *Inventor Holdings v. Bed Bath Beyond*.[25] Similar to the claimed system, the claims at issue in *Inventor Holdings* provided functionality for a customer to make a purchase from a merchant by paying a third party (in that instance, a local merchant that allowed a customer to pay in person, presumably in cash, in order to keep their credit card information safe).[26] Rejecting an argument that the claims included an inventive step by solving a problem through the use of computer technology, the court in *Inventor Holdings* held:

> The patent only makes generic references to computers that are not sufficient to render the claims patentable. These limitations are not sufficient to make an abstract idea patentable. The Federal Circuit explained that "[s]imply adding a 'computer aided' limitation to a claim covering an abstract concept, without more, is insufficient to render the claim patent eligible." *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333. "To salvage an otherwise patent-ineligible process, a computer must be integral to the claimed invention, facilitating the process in a way that a person making calculations or computations could not." *Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Canada (U.S.)*, 687 F.3d 1266, 1278 (Fed. Cir. 2012).[27]

Unlike the claims at issue in *Inventor Holdings*, the secure server and computer processing steps recited in the claims are integral to the claimed invention, thereby "facilitating the process in a way that a person making calculations or computations could not." In a conventional transaction, a payer provides financial account information directly to a merchant server and the merchant is then required to safeguard that sensitive financial account information. The claimed secure server and computer processing steps eliminate the need for the merchant to safeguard that sensitive financial account information by establishing a

[25] *Inventor Holdings v. Bed Bath & Beyond*, 123 F.Supp.3d 557 (D. Del. 2015) *aff'd without opinion* 643 Fed.Appx. 1014 (Fed. Cir. 2016)
[26] *Inventor Holdings*, 123 F.Supp.3d at 561
[27] *Inventor Holdings*, 123 F.Supp.3d at 562

communications link with the payer (to securely receive sensitive financial account information provided by the payer), providing an electronic data token (representing the payer's financial account information) to the merchant server (without providing the underlying financial account information to the merchant server or providing the electronic data token to the payer), and processing the payment using the payer's financial account information. In some embodiments, the merchant server can then use a representation of that electronic data token to instruct the secure server to process additional transactions using the payer's financial account information (as further recited in dependent claims 2 and 17).

The secure server and computer processing steps recited in the claims are integral to the claimed invention because they are the inventive step that differentiates the claimed invention from a conventional transaction between a customer and a merchant. And they facilitate the process, enabling the merchant to process payments using the payer's financial account information without receiving (and, therefore, having to safeguard) that sensitive financial account information, in a way that a person making calculations or computations could not.

D. Step 2B: Additionally, the specific technical features recited in the claims also amount to "significantly more" than "a mere instruction to apply" the abstract idea of *processing a payment from a payer to a payee* "on a computer"

Claims directed to a judicial exception under § 101 are nevertheless patent eligible if the claims recite "significantly more" than an instruction to apply the judicial exception. "Courts have held computer-implemented processes not to be significantly more than an abstract idea (and thus ineligible) where the claim as a whole amounts to nothing more than generic computer functions merely used to implement an abstract idea, such as an idea that could be done by a human analog (i.e., by hand or by merely thinking). On the other hand, courts have held computer-implemented processes to be significantly more than an abstract idea (and thus patent eligible), where generic computer components are able in combination to perform functions that are not merely generic."[28]

In *DDR Holdings*, for example, the Federal Circuit held that claims were patent eligible "because they do not merely recite the performance of some business practice known from the

[28] MPEP 2106.05(d)(II) citing *DDR Holdings, LLC v. Hotels.com, LP*, 773 F. 3d 1245, 1257-59 (2014)

pre-Internet world along with the requirement to perform it on the Internet. Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks."[29] There, the specific issue was that, "upon the click of an advertisement for a third-party product displayed on a host's website, the host website would lose that visitor as he or she is "transported to the third party's website." To solve that problem, the claims were directed to "an automatically-generated hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website related to the clicked advertisement. In this way, rather than instantly losing visitors to the third-party's website, the host website can instead send its visitors to a web page on the outsource provider's server that 1) incorporates 'look and feel' elements from the host website, and 2) provides visitors with the opportunity to purchase products from the third-party merchant without actually entering that merchant's website."[30]

As stated in the MPEP, claims that "amount to more than merely instructing that the abstract idea should be applied on the Internet," [31] for example claims that "specify ***how*** interactions with the Internet are manipulated to yield a desired result",[32] may provide a sufficient inventive concept to render claims patent eligible.

Like the claims at issue in *DDR*, the pending claims "do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet." Instead, like the claims at issue in *DDR*, the pending claims recite specific technical features that "specify how interactions with the Internet are manipulated to yield a desired result". Like the claims at issue in *DDR*, the pending claims "overcome a problem specifically arising in the realm of computer networks" – namely that, to process a payment online using conventional technology, merchants need to receive sensitive financial account information. Finally, like the claims at issue in *DDR*, the claimed solution to that problem is rooted in computer technology – specifically, a secure server that, in response to an electronically-generated payment transaction instruction from a merchant server, establishes a

[29] *DDR*, 773 F.3d at 1257.
[30] *Id.* at 1257-1258(internal footnote omitted)
[31] MPEP 2106.05(f)
[32] MPEP 2106.05(d)(emphasis in original) citing *DDR*, 773 F.3d at 1258

communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer). Accordingly, because the electronic data token is non-sensitive, the claimed secure server allows the merchant to conduct a transaction without the need to receive, store, and safeguard sensitive financial information of the purchaser.[33]

The pending Office Action argues that the claims "amount to mere instructions to implement" the abstract idea of processing a payment from a payer to a payee "on a computer." However, the abstract idea of processing a payment from a payer to a payee can be performed on a computer without the secure server and processing steps recited in the claims. The pending Office Action also characterizes the claimed processing steps as "insignificant extra-solution activity."[34] However, those processing steps not "incidental to the primary process" or "merely a nominal or tangential addition to the claim." Instead, those processing steps are the inventive step that differentiates the claimed invention from a conventional transaction where a payer provides financial account information directly to a merchant server.

Accordingly, the Applicant respectfully submits that the pending claims are patent eligible subject matter under § 101.

[33] Note that, in embodiments where the communications link between the secure server and the payer "is a widget or window within a website provided by the merchant server" (dependent claims 9 and 24), the claimed solution is even more like the solution in *DDR* in that it is "an automatically-generated hybrid web page that combines visual 'look and feel' elements" from the merchant server website and functionality to provide financial account information to the third-party secure server. In those embodiments, the merchant server sends its visitors to a website "that 1) incorporates 'look and feel' elements from the [merchant server] website, and 2) provides visitors with the opportunity" to submit sensitive financial account information to the third-party secure server "without actually entering" that secure server's website.

[34] "The term 'extra-solution activity' can be understood as activities incidental to the primary process or product that are merely a nominal or tangential addition to the claim. Extra-solution activity includes both pre-solution and post-solution activity." MPEP 2106.05(g)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

27557 7590 12/10/2021

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER	
MACCAGNO, PIERRE L	

ART UNIT	PAPER NUMBER
3697	

NOTIFICATION DATE	DELIVERY MODE
12/10/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

WashingtonDocketing@blankrome.com
jyeddo@BlankRome.com

Office Action Summary	Application No. 16/535,424	Applicant(s) POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3697	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 9-9-2021.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-46 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-46 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8-8-2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Status of Claims

1. This action is a final rejection.
2. Claims 1-46 are pending
3. Claims 1-12; 14-25 were amended
4. Claims 26-46 were added
5. Claims 1-46 are rejected under **35 USC § 101**

Priority

Acknowledgement is made of Applicant's claim for a domestic priority date of 6-5-2012.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 8-8-2019, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims **[1-46]** are not patent eligible because the claimed invention is directed to an abstract idea without significantly more.

Analysis

First, claims are directed to one or more of the following statutory categories: a process, a machine, a manufacture, and a composition of matter. Regarding claims **1-46**, the claims recite an abstract idea of processing a payment from a payer to a payee.

Independent Claims 1 and 16 are rejected under 35 U.S.C 101 based on the following analysis.

-Step 1 (Does the claim fall within a statutory category? YES): claims 1 and 16 recite a method, system and non-transitory computer readable storage medium for processing a payment from a payer to a payee.

-Step 2019 PEG 2A Prong One (Does the claim fall within at least one of the groupings of abstract ideas?: YES): The claimed invention "the payment transaction instruction including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee"; "establishing a communications link for the payer to receive financial account"; "providing an electronic data token representing the financial account information provided by the payer to the merchant… without providing the financial account information to the merchant …and without providing the electronic data token to the payer"; "processing the payment using the financial account information provided by the payer"and "forwarding at least a portion of the amount of the payment to the payee"; falls under the grouping of certain methods of organizing human activity under fundamental economic practices as it recites processing a payment from a payer to a payee. (refer to MPEP 2106.04(a)(2)). Accordingly this claim recites an abstract idea.

-Step 2019 PEG 2A Prong Two (Are there additional elements in the claim that imposes a meaningful limit on the abstract idea? NO). Claims 1 & 16 recite: "secure server"; "merchant server"; In addition claim 16 recites: "one or more processors"; and memory storing instructions "; amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea. (refer to MPEP 2106.05(f))

Claims 1 and 16 also recite: "receiving an electronically-generated payment transaction instruction"; "receiving the financial account information provided by the payer"; and "storing the financial account information provided by the payer"; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering and storing. (refer to MPEP 2106.05(g). Accordingly, the claim as a whole does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea.

-Step 2019 PEG 2B (Does the additional elements of the claim provide an inventive concept?: NO. As discussed previously with respect to Step 2A Prong Two, Claims 1 & 16 recite: "secure server"; "merchant server"; In addition claim 16 recites: "one or more processors"; and memory storing instructions "; amount to mere instructions to

implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea (refer to MPEP 2106.05(f))

Claims 1 and 16 also recite: "receiving an electronically-generated payment transaction instruction"; "receiving the financial account information provided by the payer"; and "storing the financial account information provided by the payer"; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering and storing. (refer to MPEP 2106.05(g). Under Step 2B further analysis under well-understood routine conventional (WURC) is required which includes consideration of the four options per the Berkheimer memo. Using WURC option 2 "receiving data"; "sending data" ; "transmitting data"; "selecting data"; "presenting data"; "storing data" or "gathering data" can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Accordingly, the claim does not provide an inventive concept (significantly more than the abstract idea) and hence the claim is ineligible.

Independent Claims 31 and 46 are rejected under 35 U.S.C 101 based on the following analysis.

-Step 1 (Does the claim fall within a statutory category? YES): claims 31 and 46 recite a method, system and non-transitory computer readable storage medium of enrolling a payer and processing their payment by a merchant for the benefit of a payee.

-Step 2019 PEG 2A Prong One (Does the claim fall within at least one of the groupings of abstract ideas?: YES): The claimed invention "generating an electronic instruction … that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a communications link …to receive financial account information provided by the payer"; "wherein the merchant… does not receive the financial account information represented by the electronic data token … does not provide the electronic data token to the payer"; and "processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token"; falls under the grouping of certain methods of organizing human activity under fundamental economic practices as it recites processing a payment from a payer to a payee. (refer to MPEP 2106.04(a)(2)). Accordingly this claim recites an abstract idea.

-Step 2019 PEG 2A Prong Two (Are there additional elements in the claim that imposes a meaningful limit on the abstract idea? NO). Claims 31 & 46 recite: "secure server"; and "outputting the electronic instruction to a communications network for transmittal

to the secure server"; In addition claim 46 recites: "one or more processors"; and non-transitory computer readable storage media"; amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea. (refer to MPEP 2106.05(f))

Claims 31 and 46 also recite: "receiving enrollment data identifying a payer"; "receiving, …, an electronic data token representing financial account information received …via the communications link"; and "storing the electronic data token in association with the enrollment data identifying the payer"; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering and storing. (refer to MPEP 2106.05(g). Accordingly, the claim as a whole does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea.

-Step 2019 PEG 2B (Does the additional elements of the claim provide an inventive concept?: NO. As discussed previously with respect to Step 2A Prong Two, Claims 31 & 46 recite: "secure server"; and "outputting the electronic instruction to a communications network for transmittal to the secure server"; In addition claim 46 recites: "one or more processors"; and non-transitory computer readable storage media"; amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea. (refer to MPEP 2106.05(f))

Claims 31 and 46 also recite: "receiving enrollment data identifying a payer"; "receiving, …, an electronic data token representing financial account information received …via the communications link"; and "storing the electronic data token in association with the enrollment data identifying the payer"; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering and storing. (refer to MPEP 2106.05(g). Under Step 2B further analysis under well-understood routine conventional (WURC) is required which includes consideration of the four options per the Berkheimer memo. Using WURC option 2 "receiving data"; "sending data" ; "transmitting data"; "selecting data"; "presenting data"; "storing data"; or "gathering data" can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Accordingly, the claim does not provide an inventive concept (significantly more than the abstract idea) and hence the claim is ineligible.

Claims 2-15, dependent on claim 1; claims 17-30 dependent on claim 16 and claims 32-45 dependent on claim 31 are rejected under 35 U.S.C 101 based on similar rationale as

claims 1, 16 and 31 respectively. The additionally recited elements in the dependent claims were all individually and collectively examined and found to merely refine and/or further limit the abstract idea(s) of the independent claim(s). They do not add any feature which integrates the judicial exception into a practical application, nor do they amount to significantly more, indicative of an inventive concept which cures the deficiencies of their respective parent independent claim or transforms the nature of the claims into patent-eligible subject matter under 35 USC §101.

Claim 2 dependent on claim 1, and claim 17 dependent on claim 16 merely adds to the abstract idea of claims 1 and 16 respectively. By reciting "including a representation of the electronic data token"; "specifying the amount of the second payment from the payer to the payee"; "processing the second payment using the financial account information represented by the electronic data token"; and "forwarding at least a portion of the second payment to the payee "; it adds to the abstract idea of processing a payment from a payer to a payee **by** specifying the amount of the second payment from the payer to the payee, and forwarding the payment to the payee **without** adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 2 dependent on claim 1 and claim 17 dependent on claim 16 merely recite additional steps that amount to no more than insignificant extra-solution activities to the judicial exception. Specifically claims 2 and 17 recite "receiving a second payment transaction instruction from the merchant server". This claim amounts to additional insignificant extra solution activities to the judicial exception specific to data gathering, which is a form of insignificant extra-solution activity (refer to MPEP 2016.05 (g). Such limitation does not integrate the abstract idea into a practical application. Further analysis under WURC option 2 "receiving data"; "sending data" ; "transmitting data"; "selecting data"; "presenting data"; or "gathering data" can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Such limitation does not amount to significantly more than an abstract idea and hence the claim is ineligible.

Claim 3 dependent on claim 2, claim 18 dependent on claim 17 and claim 32 dependent on claim 31 merely adds to the abstract idea of claims 1, 16 and 31 respectively. By reciting "the representation of the electronic data token is the electronic data token"; it adds to the abstract idea of processing a payment from a payer to a payee **by** defining

the representation of the electronic data token to be the electronic data token **without** adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 4 dependent on claim 1, claim 19 dependent on claim 17 and claim 33 dependent on claim 31 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claim 1, 16 and 31 respectively by reciting "wherein the payment transaction instruction is generated by the merchant server using an application programming interface provided to the merchant server by the secure server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 5 dependent on claim 4 and claim 20 dependent on claim 19 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1 and 16 respectively by reciting "wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 6 dependent on claim 4, claim 21 dependent on claim 19, and claim 34 dependent on claim 33 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1, 16 and 31 respectively, by reciting "wherein the application programming interface is implemented within a website hosted by the merchant server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 7 dependent on claim 4, claim 22 dependent on claim 19, and claim 35 dependent on claim 33 merely adds to the abstract idea of claims 1, 16 and 31 respectively. By reciting "wherein the at least one data element associated with the payer is a customer identification number … to identify the payer"; it adds to the abstract idea of processing a payment from a payer to a payee **by** defining at least one data element associated with the payer is a customer identification number …to identify the payer **without** adding any additional elements that impose a meaningful limit on the abstract idea or

any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 8 dependent on claim 1, claim 23 dependent on claim 16, and claim 36 dependent on claim 31 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1, 16 and 31 respectively, by reciting "wherein the communications link is a secure conection via the internet between the secure server and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the secure server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 9 dependent on claim 8, claim 24 dependent on claim 23, and claim 37 dependent on claim 36 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1, 16 and 31 respectively, by reciting "the secure connection is a widget or window within a website provided by the merchant server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 10 dependent on claim 8, claim 25 dependent on claim 23, and claim 38 dependent on claim 36 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1, 16 and 31 respectively, by reciting "wherein the secure connection is established via a static or dynamic uniform resource locator (URL)". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 11 dependent on claim 8, claim 26 dependent on claim 23, and claim 39 dependent on claim 36 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims 1, 16 and 31 respectively, by reciting "wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 12 dependent on claim 1, claim 27 dependent on claim 16, and claim 40 dependent on claim 31 amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claims

1, 16 and 31 respectively, by reciting "wherein the communications link used by the secure server to receive the financial account information provided by the payer is synchronous or asynchronous with a process performed by the merchant server, to receive enrollment data provided by the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 13 dependent on claim 1, claim 28 dependent on claim 16, and claim 42 dependent on claim 31 merely adds to the abstract idea of claims 1, 16 and 31 respectively. By reciting "wherein the financial account information includes at least one of a credit card number or bank account number"; it adds to the abstract idea of processing a payment from a payer to a payee **by** specifying that the financial account information includes at least a credit card number or bank account number **without** adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 14 dependent on claim 1, claim 29 dependent on claim 1, and claim 43 dependent on claim 31 merely add to the abstract idea of claims 1, 16 and 31 respectively. By reciting "wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information"; it adds to the abstract idea of processing a payment from a payer to a payee **by** specifying that merchant transactions are to be processed using the financial account information without transmitting, processing or storing the financial account information **without** adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 15 dependent on claim 1, claim 30 dependent on claim 16, and claim 44 dependent on claim 31 merely add to the abstract idea of claims 1, 16 and 31 respectively. By reciting "wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information"; it adds to the abstract idea of processing a payment from a payer to a payee **by** specifying that merchant transactions are to be processed using the financial account information without transmitting, processing or storing the financial account information **without** adding any additional

elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 41 dependent on claim 31 merely recites additional steps that amount to no more than insignificant extra-solution activities to the judicial exception. Specifically claim 41 recites: "wherein the enrollment data identifying the payer is received from the payer over a network". This claim amounts to additional insignificant extra solution activities to the judicial exception specific to data gathering, which is a form of insignificant extra-solution activity (refer to MPEP 2016.05 (g). Such limitation does not integrate the abstract idea into a practical application. Further analysis under WURC option 2 "receiving data"; "sending data" ; "transmitting data"; "selecting data"; "presenting data"; or "gathering data" can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Such limitation does not amount to significantly more than an abstract idea and hence the claim is ineligible.

Claim 45 dependent on claim 31, amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea of claim 31, by reciting "wherein the payment processing system is the secure server". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim Rejections - 35 USC § 101-Double Patenting

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims **1, 8-10, 12-13, 16, 23-25, 27-28, 31-38, 40-42 and 46** of this application are patentably indistinct from claims **1-4, 10-11 and 18-19** of Patent No. 10423940 B2 filed 1-17-2017.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not

patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

- Claims 1 and 16 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1, 15 and 26 of U.S. Patent No. 10423940 B2 to Pollin.

  Patent claims 1, 15 and 26 of Pollin 10423940 B2 recite:
  - receive enrollment data identifying a payer;
  - generate an electronic instruction for a second computing system that includes at least one data element associated with the payer and specifies a communications link for the second computing system to obtain financial account information from the payer;
  - output the electronic instruction to a communications network for transmittal to the second computing system;

- receive an electronic data token representing the financial account information obtained by the second computing system via the specified communications link from the second computing system, wherein the first computing system does not receive the financial account information represented by the electronic data token and the second computing system does not provide the electronic data token to the payer;
- store the electronic data token in association with the enrollment data identifying the payer; and
- process a payment from the payor to the payee by electronically generating a payment transaction instruction that includes a representation of the electronic data token and electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token.

Although Pollin teaches limitations 2-6 and partially teaches limitation 1 of claims 1 and 16, Pollin does not explicitly teach limitation 1 in its entirety or limitation 7 of claims 1 and 16. It would have been obvious to one of ordinary skill in the art to have modified claim 1 and 16 of Pollin to include "specifying the amount of the payment from the payer to the payee" and "forwarding at least a portion of the payment to the payee" since based on limitations 2-6 the amount of payment sent is implicit and forwarding the payment to the payee is interpreted by Examiner as being part of processing the payment. Therefore, the claim would have been obvious because "a person of ordinary skill has a good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense." *KSR Int'l Co. v. Teleflex Inc. 82 USPQ2d 1385, 1397.*

- Claims 31 and 46 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1, 15 and 26 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 31, and 46 are anticipated by patent claims 1, 15 and 26.

Patent claims 1, 15 and 26 of Pollin 10423940 B2 recite:

- receive enrollment data identifying a payer;
- generate an electronic instruction for a second computing system that includes at least one data element associated with the payer and specifies a

communications link for the second computing system to obtain financial account information from the payer;

- output the electronic instruction to a communications network for transmittal to the second computing system;
- receive an electronic data token representing the financial account information obtained by the second computing system via the specified communications link from the second computing system, wherein the first computing system does not receive the financial account information represented by the electronic data token and the second computing system does not provide the electronic data token to the payer;
- store the electronic data token in association with the enrollment data identifying the payer; and
- process a payment from the payor to the payee by electronically generating a payment transaction instruction that includes a representation of the electronic data token and electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token.

Therefore patent claims 1, 15 and 26 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 31, and 46. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

- Claims 8, 23 and 36 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 4, and 17 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 8, 23, and 36 are anticipated by patent claims 4, and 17.

Patent claims 4 and 17 of Pollin 10423940 B2 recite:

- wherein the communication link is a secure connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system

Therefore patent claims 4 and 17 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 8, 23 and 36. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

- Claims 9, 24 and 37 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 5 and 18 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 9, 24, and 37 are anticipated by patent claims 5, and 18.

  Patent claims 5, and 18 of Pollin 10423940 B2 recite:
  - wherein the secure connection is a widget or window within a website provided by the first computing system

  Therefore patent claims 5 and 18 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 9, 24 and 37. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

- Claims 10, 25 and 38 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 6 and 19 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 10, 25, and 38 are anticipated by patent claims 6, and 19.

  Patent claims 6, and 19 of Pollin 10423940 B2 recite:
  - wherein the secure connection provides access to the second computing system using a static or dynamic universal resource locator (URL)

  Therefore patent claims 6 and 10 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 10, 25 and 38. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

- Claims 12, 27 and 40 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 2 & 16 and 7 & 20 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 12, 27, and 40 are anticipated by patent claims 2 & 16 and 7 & 20.

  Patent claims 2 & 16 of Pollin 10423940 B2 recite:
  - wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used to obtain the enrollment data

  Patent claims 7 & 20 of Pollin 10423940 B2 recite:
  - wherein the communications link used to obtain the financial account information from the payer is asynchronous with a communications link used to obtain the enrollment data

  Therefore patent claims 2 & 16 and 7 & 20 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 12, 27 and 40. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

- Claims 13, 28 and 42 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 13 and 24 of U.S. Patent No. 10423940 B2 to Pollin. Although the claims at issue are not identical, they are not patentably distinct from each other because application claims 13, 28, and 42 are anticipated by patent claims 13, and 24.

  Patent claims 13, and 24 of Pollin 10423940 B2 recite:
  - wherein the financial account information includes at least one of a credit card number or bank account number

  Therefore patent claims 13 and 24 of Pollin 10423940 B2 are in essence a "species" of the generic invention of application claims 13, 28 and 42. It has been held that a generic invention is "anticipated" by a "species" within the scope of the generic invention. See In re Goodman, 29 USPQ2d 2010 (Fed. Cir. 1993).

Response to Arguments

Applicant's arguments filed 9/9/2021 have been fully considered but they are not persuasive. (FP **7.37**)

Applicant amended independent claims 1, and 16 and dependent claims 2-12, 14-15 and 17-25, in addition to adding claims 26-46 as posted in the above analysis with additions underlined. Deletions were not shown as ~~strike through text~~ because of the sizeable amount of them

In response to applicant's arguments regarding claim rejection under 35 U.S.C § 101:

Step 2A Prong One: Applicant does not argue against the claims being directed to an abstract idea. According to the analysis under step 2A prong one, the selected claim recitation belongs to the grouping of certain methods of organizing human activity under fundamental economic practices as it recites processing a payment from a payer to a payee. (refer to MPEP 2106.04(a)(2)). Accordingly this claim recites an abstract idea.

Step 2A Prong Two and Step 2B : Applicant argues that even if the claims were directed to an abstract idea the specific claims constitute “significantly more” since the claim recites a “practical application” and “invention concept” that imposes meaningful limits related to the processing of a payment from a payer to a payee on the judicial exception.

Specifically Applicant argues that the claims "impose a meaningful limit" on the broad concept of processing a payment by reciting specific technical features - namely, a secure server that, in response to an electronically-generated payment transaction instruction from a merchant server (including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee), establishes a communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer). The Applicant further argues that those specific technical features direct the claim to a specific, practical application and inventive concept of that broad concept - namely, processing a transaction from a payer to a payee without the payee having access to (or being required to secure) the underlying financial account information in addition to allowing the merchant to conduct a transaction without the need to receive, store, and

safeguard sensitive financial information of the purchaser based on the non-sensitive electronic data token, and the claimed secure server

The Examiner disagrees. Several of the points that the Applicant claims "impose a meaningful limit" are included as part of the abstract idea under Step 2A Prong One and were not listed as additional elements. Furthermore, as explained under the PEG2A Prong Two analysis, all the listed additional recited elements: "secure server"; "merchant server"; "outputting the electronic instruction to a communications network for transmittal to the secure server"; "one or more processors"; and non-transitory computer readable storage media"; amount to no more than mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea (refer to MPEP 2106.05(f)). In addition the recited insignificant extra solution activity to the judicial exception: "receiving enrollment data identifying a payer"; "receiving, …, an electronic data token representing financial account information received …via the communications link"; and "storing the electronic data token in association with the enrollment data identifying the payer" specific to receiving and storing data as listed in the analysis do not amount to an inventive concept, particularly when the activity is well understood routine conventional (refer to MPEP 2106.05(g) and (see MPEP 2106.05 (d)(II)). Accordingly the claim as a whole does not integrate the abstract idea into a practical application or an inventive concept because it does not impose any meaningful limits on practicing the abstract idea and hence the claims remain rejected under 35 U.S.C. 101.

In conclusion for reasons of record and as set forth above, the examiner maintains the rejection of claims **1-46** as being directed to a judicial exception without significantly more, and thereby being directed to non-statutory subject matter under 35 USC §101. In addition, the examiner rejects claims **1, 8-10, 12-13, 16, 23-25, 27-28, 31-38, 40-42 and 46** under 35 USC § 101 non statutory double patenting as being patentably indistinct from claims **1-4, 10-11 and 18-19** of Patent No. 10423940 B2 based on the amendments and additions made by the Applicant. In reaching this decision, the Examiner considered all evidence presented and all arguments actually made by Applicant.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE L MACCAGNO whose telephone number is (571)270-5408. The examiner can normally be reached on M-F 8:00 to 5:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, supervisory patent examiner, Christine Behncke can be reached at 571-272-8103. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PIERRE L MACCAGNO/
Examiner, Art Unit 3697

/CHRISTINE M BEHNCKE/
Supervisory Patent Examiner, Art Unit 3697

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3697	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20020107791-A1	08-2002	Nobrega, Ryan J.	G06Q20/327	705/39
*	B	US-20120078799-A1	03-2012	JACKSON; James	G06Q20/12	705/67
*	C	US-7120609-B1	10-2006	Kerkdijk; Hendrikus	G06Q20/02	705/78
*	D	US-20090240594-A1	09-2009	Kerner; Robert	G06Q30/0601	705/26.1
*	E	US-20080083826-A1	04-2008	Henry; James M.	G06Q20/10	235/379
*	F	US-20140074695-A1	03-2014	BARKAN; Mordhay	G06Q20/3674	705/39
*	G	US-20190362324-A1	11-2019	POLLIN; Robert Evan	G06Q20/10	1/1
*	H	US-7801825-B2	09-2010	Kranzley; Arthur D.	G06Q20/3821	705/67
*	I	US-20010056402-A1	12-2001	Ahuja, Arun	G06Q20/1085	705/43
*	J	US-20020087704-A1	07-2002	Chesnais, Pascal	H04L69/329	709/228
*	K	US-20130198080-A1	08-2013	Anderson; Lisa	G06Q20/26	705/44
*	L	US-20040143550-A1	07-2004	Creamer, Thomas E.	G06Q20/105	705/41
*	M	US-20050197962-A1	09-2005	Critchfield, Steve Taylor	G06Q50/26	705/53

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3697	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20090048953-A1	02-2009	Hazel; Patrick	G07F7/1008	705/35
*	B	US-20090132351-A1	05-2009	Gibson; Garry H.	G06Q20/02	705/12
*	C	US-20110029436-A1	02-2011	Norvell; Joel	H04L63/08	705/67
*	D	US-20110078244-A1	03-2011	Minter; David D.	G06Q30/02	709/204
*	E	US-20110184853-A1	07-2011	Mark; Timothy James	G06Q20/3221	705/39
*	F	US-20120023567-A1	01-2012	Hammad; Ayman	G06Q20/4016	726/9
*	G	US-20120030066-A1	02-2012	Stringfellow; Westley	G06Q20/40	705/26.41
*	H	US-20120259782-A1	10-2012	Hammad; Ayman	G06Q20/382	705/44
*	I	US-20100235286-A1	09-2010	Moore; Daryl Richard	G06Q10/107	705/76
*	J	US-20110029416-A1	02-2011	Greenspan; Aaron J.	G06Q30/0611	705/30
*	K	US-20020165821-A1	11-2002	Tree, Ian David	G06Q20/04	705/39
*	L	US-20070011093-A1	01-2007	Tree; Ian David	G06Q20/10	705/40
*	M	US-20090063353-A1	03-2009	Viidu; Siim	G06Q20/16	705/75

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3697	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7680736-B2	03-2010	Jarman; Jonathan S.	G06Q20/202	705/41
*	B	US-20110161233-A1	06-2011	Tieken; Craig A.	G06Q20/4014	705/71
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN, Robert Evan
	Examiner	Art Unit
	PIERRE L MACCAGNO	3697

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/10	03/12/2021	PM
G06Q20/10; G06Q10/107; G06Q20/102; G06Q20/12; G06Q20/305; G06Q20/40; G06Q20/4014; G06Q10/00	11/26/2021	PM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
G06Q20/10	03/12/2021	PM
East Text Search	03/12/2021	PM
Dialog NPL search	03/12/2021	PM
G06Q20/10; G06Q10/107; G06Q20/102; G06Q20/12; G06Q20/305; G06Q20/40; G06Q20/4014; G06Q10/00	11/26/2021	PM
Updated "Search" text search	11/26/2021	PM
Updated Dialog NPL search	11/26/2021	PM

/PIERRE L MACCAGNO/ Examiner, Art Unit 3697	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN, Robert Evan
	Examiner	Art Unit
	PIERRE L MACCAGNO	3697

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PIERRE L MACCAGNO/ Examiner, Art Unit 3697	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN et al.
	Examiner	Art Unit
	PIERRE L MACCAGNO	3697

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/12/2021	10/23/2021							
1	1	✓	✓							
2	2	✓	✓							
3	3	✓	✓							
4	4	✓	✓							
5	5	✓	✓							
6	6	✓	✓							
7	7	✓	✓							
8	8	✓	✓							
9	9	✓	✓							
10	10	✓	✓							
11	11	✓	✓							
12	12	✓	✓							
13	13	✓	✓							
14	14	✓	✓							
15	15	✓	✓							
16	16	✓	✓							
17	17	✓	✓							
18	18	✓	✓							
19	19	✓	✓							
20	20	✓	✓							
21	21	✓	✓							
22	22	✓	✓							
23	23	✓	✓							
24	24	✓	✓							
25	25	✓	✓							
26			✓							
27			✓							
28			✓							
29			✓							
30			✓							
31			✓							
32			✓							
33			✓							
34			✓							
35			✓							
36			✓							
37			✓							
38			✓							
39			✓							
40			✓							
41			✓							
42			✓							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/535,424	POLLIN et al.
	Examiner	**Art Unit**
	PIERRE L MACCAGNO	3697

CLAIM		DATE								
Final	Original	03/12/2021	10/23/2021							
43			✓							
44			✓							
45			✓							
46			✓							

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	12	autoscribe.as.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/10 09:49 PM
L2	10	autoscribe.as. and (pollin).in.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/10 09:54 PM
L3	102	"7801825" "20090132351" "20010056402" "20020087704" "20040143550" "20050197962" "20070250920" "20110029436" "20110078244" "20120030066" "20020107791" "20110184853" "20120023567" "20120259782" "20130198080" "20090048953" "20060235796"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/10 09:59 PM
L4	4147	payment with process$3 with transaction with first with second	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 06:43 AM
L5	201	payment with process$3 with transaction with first with second with token	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 06:44 AM
L6	19	(payment with process$3 with transaction with first with second with token)and (G06Q20/10).CPC.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 06:45 AM
L7	45	(payment with transaction with first with second with token)and (G06Q20/10).CPC.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 06:49 AM
L8	49	("2011/0029416").URPN.	(USPAT)	OR	ON	ON	2021/03/11 07:00 AM
L9	2	(aaron same greenspan).IN.	(USPAT)	OR	ON	ON	2021/03/11 07:02 AM
L10	272	(payment with process$3 with transaction with first with second)same	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:05 AM

		token					
L11	28	((payment with process$3 with transaction with first with second)same token)and(G06Q20/10). CPC.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:06 AM
L12	60	((payment with transaction with first with second) same token)and (G06Q20/10).CPC.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:12 AM
L13	138	((payment with first with second) same token)and (G06Q20/10).CPC.	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:44 AM
L14	13	((payment with first with second) same token)and (G06Q20/10).CPC. and @py<"2013"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:53 AM
L15	13	((payment with first with second) same token)and (G06Q20/10).CPC. and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:54 AM
L16	830	(payment with process$3 with transaction with first with second) and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:57 AM
L17	154	(payment with process$3 with transaction with first with second) and token and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 07:58 AM
L18	426	(payment with transaction with first with second) and token and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 08:00 AM
L19	1689	(payment with first with second) and token and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 08:00 AM
L20	310	(payment with first with second) and token and (G06Q20/10).CPC. and @py<="2012"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 08:01 AM
L21	310	((payment with first with second) and token)and (G06Q20/10).CPC. and @py<"2013"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/11 08:13 AM
L22	427	((payment) with token)and (G06Q20/10).CPC. and	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/12 01:18 PM

		@py<"2013"					
L23	5	((payment) with (data adj token))and (G06Q20/10).CPC. and @py<"2013"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/12 02:10 PM
L24	24	((payment) with ((data or transaction) adj token))and (G06Q20/10).CPC. and @py<"2013"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT)	OR	ON	ON	2021/03/12 02:13 PM
L25	28	(payee WITH payer) SAME token SAME (communication$1 WITH link)	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/25 05:44 PM
L26	14	(payee WITH payer) SAME token SAME (communication$1 WITH link) AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/25 05:48 PM
L27	219	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO;	OR	ON	ON	2021/11/25 05:57 PM

			JPO; DERWENT; IBM_TDB)				
L28	95	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME (token WITH (communication$1 WITH (link OR connection OR interface OR interconnection))) AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/25 06:07 PM
L29	14	"10423940"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:17 AM
L30	27	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/10).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:49 AM
L31	2	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS,	OR	ON	ON	2021/11/26 11:50 AM

		WITH (link OR connection OR interface OR interconnection)) AND (G06Q10/107).CPC. AND @py<= "2012"	IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L32	23	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/102).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:51 AM
L33	34	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/12).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:52 AM
L34	0	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/305).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:52 AM

L35	52	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/40).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:53 AM
L36	12	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q20/4014).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:53 AM
L37	0	((payee OR recipient OR merchant) WITH (payer OR client OR customer OR purchaser OR buyer)) SAME token SAME (communication$1 WITH (link OR connection OR interface OR interconnection)) AND (G06Q10/00).CPC. AND @py<= "2012"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/11/26 11:54 AM
L38	34	(US-20010056402-$ | US-20020087704-$ | US-20020107791-$ | US-20040143550-$ | US-20050197962-$ | US-20060235796-$ | US-20070250920-$ | US-20090048953-$ | US-20090132351-$ |	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL,	OR	ON	ON	2021/11/26 12:11 PM

		US-20110029436-$ | US-20110078244-$ | US-20110184853-$ | US-20120023567-$ | US-20120030066-$ | US-20120259782-$ | US-20130198080-$ | US-7801825-$).DID.	NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Robert E. Pollin
Art Unit	
Examiner Name	
Attorney Docket Number	124452-00122

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7801825		2010-09-21	Kranzley et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090132351	A1	2009-05-21	Gibson	
	2	20010056402	A1	2001-12-27	Ahuja et al.	
	3	20020087704	A1	2002-07-04	Chesnais et al.	
	4	20040143550	A1	2004-07-22	Creamer et al.	
	5	20050197962	A1	2005-09-08	Critchfield et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.L.M./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

	6	20070250920	A1	2007-10-25	Lindsay	
	7	20110029436	A1	2011-02-03	Norvell et al.	
	8	20110078244	A1	2011-03-31	Minter et al.	
	9	20120030066	A1	2012-02-02	Stringfellow et al.	
	10	20020107791	A1	2002-08-08	Nobrega et al.	
	11	20110184853	A1	2011-07-28	Mark et al.	
	12	20120023567	A1	2012-01-26	Hammad	
	13	20120259782	A1	2012-10-11	Hammad	
	14	20130198080	A1	2013-08-01	Anderson et al.	
	15	20090048953	A1	2009-02-19	Hazel	
	16	20060235796	A1	2006-10-19	Johnson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.L.M./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/PIERRE L MACCAGNO/	Date Considered	03/10/2021

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.L.M./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	
Name/Print	Michael C. Greenbaum	Registration Number	28419

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.L.M./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /P.L.M./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert Evan POLLIN et al.

Application No.: 16/535,424 | Confirmation No.: 2047

Filed: August 8, 2019 | Art Unit: 3696

For: PROCESSING A PAYMENT BY A SECOND COMPUTING SYSTEM FROM A PAYER TO A PAYEE OPERATING A FIRST COMPUTING SYSTEM | Examiner: Pierre L. MACCAGNO

AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated March 17, 2021, please amend the above-identified U.S. patent application as follows:

Amendment to the Title begins on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Remarks/Arguments begin on page 16 of this paper.

AMENDMENT TO THE TITLE

Please amend the title as follows:

ENROLLING A PAYER BY A MERCHANT SERVER OPERATED BY OR FOR THE BENEFIT OF A PAYEE AND PROCESSING A PAYMENT FROM THE PAYER BY A SECURE SERVER~~SECOND COMPUTING SYSTEM FROM A PAYER TO A PAYEE OPERATING A FIRST COMPUTING SYSTEM~~

AMENDMENTS TO THE CLAIMS

1. (Currently Amended): A method of processing a payment from a payer to a payee ~~operating a first computing system~~, the method being performed by a ~~second computing system~~secure server, the method comprising:

receiving an electronically-generated payment transaction instruction from ~~the first computing system~~a merchant server, ~~wherein~~ the payment transaction instruction ~~includes~~ including at least one data element associated with the payer~~, specifies~~ and specifying the amount of the payment from the payer to the payee; ~~and~~

establishing ~~specifies~~ a communications link with the payer ~~for the second computing system~~ to ~~obtain~~ receive financial account information ~~from~~ provided by the payer;

receiving ~~obtaining~~ the financial account information ~~from~~ provided by the payer via the ~~specified~~ communications link;

providing ~~generating~~ an electronic data token, representing the financial account information ~~obtained from~~provided by the payer~~, outputting the electronic data token to a communications network for transmittal~~ to the merchant server ~~first computing system, wherein the first computing system does not receive~~ without providing the financial account information to the merchant server and ~~the second computing system does not provide~~ without providing the electronic data token to the payer;

storing the financial account information ~~obtained from~~ provided by the payer;

~~obtaining the amount of the payment from the payer by~~ processing the payment using the financial account information ~~obtained from~~provided by the payer; and

forwarding at least a portion of ~~the amount of~~ the payment to the payee.

2. (Currently Amended): The method of claim 1, further comprising:

receiving a second payment transaction instruction from the ~~first computing system~~ merchant server, ~~wherein~~ the second payment transaction instruction ~~includes~~ including a representation of the electronic data token~~, and specifies~~ and specifying the amount of the second payment from the payer to the payee;

processing the second payment using the financial account information represented by the electronic data token; and

forwarding ~~the amount~~ at least a portion of the second payment to the payee.

3. (Currently Amended): The method of claim 2, wherein the representation of the electronic data token is the electronic data token~~claim 1, wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used by the first computing system to obtain enrollment data from the payer~~.

4. (Currently Amended): The method of claim 1, wherein the payment transaction instruction is generated by the merchant server using an application programming interface provided to the merchant server by the secure server~~the communications link is at least one of a telephone number to enable the second computing system to communicate with the payer and obtain the financial account information or a transfer from an existing telephone call with the payer to a telephone system that receives the financial account information from the payer~~.

5. (Currently Amended): The method of claim 4, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server~~claim 1, wherein the communication link is a connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system~~.

6. (Currently Amended): The method of claim 4, wherein the application programming interface is implemented within a website hosted by the merchant server~~claim 5, wherein the connection is a widget or window within a website provided by the first computing system~~.

7. (Currently Amended): The method of claim 4, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payerclaim 5, wherein the connection provides access to the second computing system using a static or dynamic universal resource locator (URL).

8. (Currently Amended): The method of claim 1, wherein the communications link is a secure connection via the internet between the secure server and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the secure serverused to obtain the financial account information from the payer is asynchronous with a communications link used by the first computing system to obtain enrollment data from the payer.

9. (Currently Amended): The method of claim 8, wherein the secure connection is a widget or window within a website provided by the merchant serverthe payment transaction instruction for the second computing system to obtain the financial account information from the payer includes data sufficient for the second computing system to authenticate the payer.

10. (Currently Amended): The method of claim 8, wherein the secure connection is established via a static or dynamic uniform resource locator (URL)claim 9, wherein the first computing system defines a period of persistence for the second computing system to obtain the financial account information from the payer.

11. (Currently Amended): The method of claim 8, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure serverclaim 1, wherein the payment transaction instruction comprises contact information for the payer to enable the second computing system to transmit instructions to the payer for communicating the financial account information to the second computing system.

12. (Currently Amended): The method of claim 1, wherein the communications link used by the secure server to receive the financial account information provided by the payer is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data provided by the payer~~claim 11, wherein the contact information comprises one of an email address or a telephone number whereby the second computing system sends a link for a data entry connection to the payer via one of email and text~~.

13. (Original): The method of claim 1, wherein the financial account information includes at least one of a credit card number or bank account number.

14. (Currently Amended): The method of claim 1, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

~~A second computing system that processes a payment from a payer to a payee operating a first computing system, the second computing system comprising:~~

~~one or more processors; and~~

~~memory storing instructions that, when executed by the one or more processors, cause the second computing system to:~~

~~receive an electronically generated payment transaction instruction from a first computing system, wherein the payment transaction instruction:~~

~~includes at least one data element associated with the payer;~~

~~specifies the amount of the payment from the payer to the payee; and~~

~~specifies a communications link for the second computing system to obtain financial account information from the payer;~~

~~obtain the financial account information from the payer via the specified communications link;~~

~~generate an electronic data token representing the financial account information obtained from the payer;~~

~~output the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer;~~

~~store the financial account information obtained from the payer;~~

~~obtain the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer; and~~

~~forward at least a portion of the amount of the payment to the payee.~~

15. (Currently Amended): The method of claim 1, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

~~The system of claim 14, wherein the instructions further cause the second computing system to:~~

~~receive a second payment transaction instruction from the first computing system, wherein the second payment transaction instruction:~~

~~includes a representation of the electronic data token; and~~

~~specifies the amount of the second payment from the payer to the payee;~~

~~obtain the amount of the second payment from the payer by processing the second payment using the financial account information represented by the electronic data token; and~~

~~forward at least a portion of the amount of the second payment to the payee.~~

16. (Currently Amended): A secure server that processes a payment from a payer to a payee, the secure server comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the secure computing system to:

receive an electronically-generated payment transaction instruction from a merchant server, the payment transaction instruction including at least one data element associated with the payer and specifying an amount of the payment from the payer to the payee,

establish a communications link with the payer to receive financial account information provided by the payer;

receive the financial account information provided by the payer via the communications link;

provide an electronic data token, representing the financial account information provided by the payer, to the merchant server without providing the financial account information to the merchant server and without providing the data token to the payer,

store the financial account information provided by the payer;

process the payment using the financial account information provided by the payer; and

forward at least a portion of the payment to the payee.

~~The system of claim 14, wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used by the first computing system to obtain enrollment data from the payer.~~

17. (Currently Amended): The secure server of claim 16, wherein the instructions further cause the secure computing system to:

receive a second payment transaction instruction from the merchant server, wherein the second payment transaction instruction includes a representation of the electronic data token and specifies an amount of a second payment from the payer to the payee;

process the second payment using the financial account information represented by the electronic data token; and

forward at least a portion of the second payment to the payee.

~~The system of claim 14, wherein the communication link is a connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system.~~

18. (Currently Amended): The secure server ~~system~~ of claim 17, wherein the representation of the electronic data token is the electronic data token~~the connection is a widget or window within a website provided by the first computing system~~.

19. (Currently Amended): The secure server of claim 16, wherein the payment transaction instruction is generated by the merchant server using an application programming interface provided to the merchant server by the secure server~~The system of claim 17, wherein the connection provides access to the second computing system using a static or dynamic universal resource locator (URL)~~.

20. (Currently Amended): The secure server of claim 19, wherein the payment transaction instruction is generated using a token retrieval function of the application programming interface provided to the merchant server by the secure server~~The system of claim 14, wherein the communications link used to obtain the financial account information from the payer is asynchronous with a communications link used by the first computing system to obtain enrollment data from the payer~~.

21. (Currently Amended): The secure server of claim 19, wherein the application programming interface is implemented within a website hosted by the merchant server~~The system of claim 20, wherein the payment transaction instruction for the second computing system to obtain the financial account information from the payer includes data sufficient for the second computing system to authenticate the payer~~.

22. (Currently Amended): The secure server of claim 19, wherein the at least one data element associated with the payer is a customer identification number generated by the merchant server to identify the payer~~The system of claim 21, wherein the first computing system defines a period of persistence for the second computing system to obtain the financial account information from the payer~~.

23. (Currently Amended): The secure server of claim 16, wherein the communication link is a secure connection via the internet between the secure server and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the secure server~~The system of claim 14, wherein the payment transaction instruction comprises contact information for the payer to enable the second computing system to transmit instructions to the payer for communicating the financial account information to the second computing system.~~

24. (Currently Amended): The secure server of claim 23, wherein the secure connection is a widget or window within a website provided by the merchant server~~The system of claim 14, wherein the financial account information includes at least one of a credit card number or bank account number~~.

25. (Currently Amended): The secure server of claim 23, wherein the secure connection is established via a static or dynamic uniform resource locator (URL).

~~A non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause a second computing system that processes a payment from a payer to a payee operating a first computing system to:~~

~~receive an electronically-generated payment transaction instruction from the first computing system, wherein the payment transaction instruction:~~

~~includes at least one data element associated with the payer;~~

~~specifies the amount of the payment from the payer to the payee; and~~

~~specifies a communications link for the second computing system to obtain financial account information from the payer;~~

~~obtain the financial account information from the payer via the specified communications link;~~

~~generate an electronic data token representing the financial account information obtained from the payer;~~

~~output the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer;~~

~~store the financial account information obtained from the payer;~~

~~obtain the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer; and~~

~~forward at least a portion of the amount of the payment to the payee.~~

26. (New): The secure server of claim 23, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

27. (New): The secure server of claim 16, wherein the communications link used by the secure server to receive the financial account information provided by the payer is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

28. (New): The secure server of claim 16, wherein the financial account information includes at least one of a credit card number or bank account number.

29. (New): The secure server of claim 16, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

30. (New): The secure server of claim 16, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

31. (New): A method of enrolling a payer by a merchant server operated by or for the benefit of a payee, the method comprising:

receiving enrollment data identifying a payer;

generating an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a communications link between the secure server and the payer for the secure server to receive financial account information provided by the payer;

outputting the electronic instruction to a communications network for transmittal to the secure server;

receiving, from the secure server, an electronic data token representing financial account information received by the secure server via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

storing the electronic data token in association with the enrollment data identifying the payer; and

processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token.

32. (New): The method of claim 31, wherein the representation of the electronic data token is the electronic data token.

33. (New): The method of claim 31, wherein the electronic instruction is generated using an application programming interface provided to the merchant server by the secure server.

34. (New): The method of claim 33, wherein the application programming interface is implemented within a website hosted by the merchant server.

35. (New): The method of claim 33, wherein the at least one data element associated with the payer is a customer identifier generated by the merchant server to identify the payer.

36. (New): The method of claim 31, wherein the communication link is a secure connection via the internet between the secure server and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the secure server.

37. (New): The method of claim 36, wherein the secure connection is a widget or window within a website provided by the merchant server.

38. (New): The method of claim 36, wherein the secure connection provides access to the secure server using a static or dynamic universal resource locator (URL).

39. (New): The method of claim 36, wherein the secure connection is established by a redirect URL that redirects the computing system used by the payer to the secure server.

40. (New): The method of claim 31, wherein the communications link used to receive the financial account information provided by the payer is synchronous or asynchronous with a process, performed by the merchant server, to receive enrollment data from the payer.

41. (New): The method of claim 31, wherein the enrollment data identifying the payer is received from the payer over a network.

42. (New): The method of claim 31, wherein the financial account information includes at least one of a credit card number or bank account number.

43. (New): The method of claim 31, wherein the electronic data token enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

44. (New): The method of claim 31, wherein the secure server enables the merchant server to process transactions using the financial account information without transmitting, processing or storing the financial account information.

45. (New): The method of claim 31, wherein the payment processing system is the secure server.

46. (New): A merchant server, operated by or for the benefit of a payee, comprising:

one or more computer processors; and

non-transitory computer readable storage media storing instructions that, when executed by the one or more computer processors, cause the merchant server to:

receive enrollment data identifying a payer;

generate an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a communications link between the secure server and the payer for the secure server to receive financial account information provided by the payer;

output the electronic instruction to a communications network for transmittal to the secure server;

receive, from the secure server, an electronic data token representing financial account information received by the secure server provided by the payer via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

store the electronic data token in association with the enrollment data identifying the payer; and

process a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and electronically transmitting the payment transaction instruction to a payment processing system having access to the financial account information represented by the electronic data token.

REMARKS

I. INTRODUCTION

The Office Action dated March 17, 2021 (hereinafter, "the pending Office Action"), has been carefully considered. In response thereto, the present application has been amended and is believed to be in condition for allowance. Accordingly, reconsideration and withdrawal of the outstanding Office Action and issuance of a Notice of Allowance are respectfully solicited in view of the following remarks.

II. STATUS OF THE CLAIMS

Claims 1-25 are pending. By way of this Amendment, claims 1-12 and 14-25 are amended and claims 26-60 are added. Support for the claim amendments may be found throughout the Applicant's Specification, for example (and without limitation) as identified below. No new matter has been added.

Claims 1, 16, 31, and 46	secure server 202 (second computing system) and merchant server 204 (first computing system)
Claims 2 and 17	Paragraph [0012]
Claims 3, 18, and 32	Paragraph [0041]
Claims 4, 19, and 33	Paragraph [0028]
Claims 5 and 20	Paragraphs [0028], [0032]
Claims 6, 21, and 34	Paragraph [0032]
Claims 7, 22, and 35	Paragraph [0048]
Claims 8, 23, and 36	Paragraph [0046]
Claims 9, 24, and 37	Paragraph [0046]
Claims 10, 25, and 38	Paragraph [0032]
Claims 11, 26, and 39	Paragraph [0046]
Claims 12, 27, and 40	Paragraph [0044]
Claims 13, 28, and 42	Paragraph [0036]
Claims 14, 29, and 43	Paragraph [0028]
Claims 15, 30, and 44	Paragraph [0028]
Claim 41	Paragraphs [0010], [0033]
Claim 45	Paragraph [0044]

III. SUMMARY OF THE OFFICE ACTION

In the pending Office Action, claims 1-25 are rejected under 35 U.S.C. § 101 as allegedly directed to non-patentable subject matter.

IV. PATENT ELIGIBLE SUBJECT MATTER REJECTION (35 U.S.C. § 101)

Merchants spend considerable time, effort, and expense securing the financial information (e.g., credit card numbers, bank account numbers) received from purchasers in order to provide a secure platform for purchasers and comply with industry security standards. The claimed invention eliminates that burden by allowing the merchant (payee) and the purchaser (payer) to conduct a transaction without the merchant receiving – and thus having to safeguard – the financial information of the purchaser.

Specifically, the claims recite a secure server [e.g., secure server 202] in communication with a merchant server [e.g., merchant server 204]. In response to an electronically-generated payment transaction instruction from the merchant server, the secure server establishes a communications link with the payer to securely receive sensitive financial account information provided by the payer. An electronic data token representing the payer's financial account information is generated. The secure server provides that electronic data token to the merchant server. Critically, the secure server provides the electronic data token without providing the underlying financial account information to the merchant server (or providing the electronic data token to the payer). The secure server and the electronic data token enable payments from a payer to payee to the processed without the payee having to receive, store, and safeguard the underlying financial account information.

In some embodiments, the secure server may provide an application programming interface (API), in some instances implemented within a website hosted by the merchant server, with functionality for the merchant server to transmit the payment transaction instruction. The communications link between the payer and the secure server may be a secure connection via the internet, such as a redirect URL. The secure connection may be a widget or window within a website provided by the merchant server, so that the process of interacting with the merchant

server while transmitting sensitive financial account information to the secure server is seamless from the viewpoint of the customer.

Because the electronic data token is non-sensitive, the merchant server may store the electronic data token (without having to comply with stringent compliance requirements) and, in some embodiments, that electronic data token may be used to process future payments authorized by the payer.

Claim 1 is directed to a method, performed by the secure server, to processes a payment from the payer to the payee by:

- receiving an electronically-generated payment transaction instruction (including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee) from the merchant server;
- establishing a communications link to receive financial account information provided by the payer;
- receiving the financial account information from the payer via the communications link;
- providing an electronic data token representing the financial account information received from the payer;
- outputting the electronic data token to a communications network for transmittal to the merchant server without providing the financial account information to the merchant server and without providing the electronic data token to the payer;
- storing the financial account information received from the payer;
- processing the payment using the financial account information obtained from the payer; and
- forwarding at least a portion of the payment to the payee.

Claim 16, which is directed to the secure server, recites analogous features.

A. The specific technical features recited in the claims "impose a meaningful limit" on the broad concept of *processing a payment from a payer to a payee* such that the claims are directed a specific, "practical application" of the broad concept (Step 2A)

"There is no dispute ... that many computer-implemented claims are formally addressed to patent-eligible subject matter."[1] Computer-implemented business methods are also patent eligible. "[A] business method is simply one kind of 'method' that is, at least in some circumstances, eligible for patenting under § 101."[2] Inventions in one of the four broad statutory categories[3] are patent eligible unless they are directed to one of "the basic tools of scientific and technological work" – namely, "laws of nature, natural phenomena, and abstract ideas"[4] – without "significantly more" than a mere instruction to apply that basic tool.[5]

Furthermore, the Supreme Court "has long distinguished between principles themselves (which are not patent eligible) and the integration of those principles into practical applications (which are patent eligible)."[6] Accordingly, even if a claim *recites* a judicial exception (Step 2A Prong One), MPEP § 2106.04(d) instructs examiners to "evaluate whether the claim as a whole integrates the recited judicial exception into a practical application of the exception." (Step 2A Prong Two). "A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception."[7] For instance, "the claimed invention may integrate the judicial exception into a practical application by demonstrating that it improves the relevant existing technology."[8]

The pending Office Action argues that the claims recite the fundamental economic practice of "processing a payment from a payer to a payee." The Applicant respectfully submits

---

[1] *Alice*, 134 S.Ct. at 2358-59 (2014)
[2] *Bilski v. Kappos*, 130 S.Ct. 3218, 3228 (2010)
[3] process, machine, manufacture, or composition of matter
[4] *Alice*, 134 S.Ct. at 2354
[5] *Id.* at 2357
[6] MPEP 2106.04(d) citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 80, 84 (2012)
[7] *Id.*
[8] MPEP 2106.04(d)(1). Note that, in Step 2A Prong One, whether the claim "pertains to" technological improvement is determined "without reference to what is well-understood, routine, conventional activity."

that *a secure server that establishes a communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer) so that the merchant server can process a transaction without having access to – or being required to secure – the underlying financial account information* is not "a fundamental economic practice."

Nevertheless, even if the claims are broadly characterized as *describing* one method of processing a payment from a payer to a payee (Step 2A Prong One), the claims can hardly be characterized as "a drafting effort designed to monopolize" the broad concept of processing a payment from a payer to a payee (Step 2A Prong Two).[9] Instead, the claims "impose a meaningful limit" on the broad concept of *processing a payment* by further reciting specific technical features – namely, a secure server that, in response to an electronically-generated payment transaction instruction from a merchant server (including at least one data element associated with the payer and specifying the amount of the payment from the payer to the payee), establishes a communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer). Those specific technical features direct the claim to a specific, practical application of that broad concept – namely, processing a transaction from a payer to a payee without the payee having access to (or being required to secure) the underlying financial account information.

The pending Office Action quotes a few of the processing steps recited in the claims and argues that those disembodied processing steps "amount to mere instructions to implement" the abstract idea of processing a payment from a payer to a payee "on a computer."[10] In doing so,

[9] Note that, if the claims *were* a drafting effort designed to monopolize the concept of processing payments, it would be quite a poor effort. One could simply and easily design around this attempted monopoly by not employing a secure server that performs the claimed processing steps. Instead, a merchant server could simply be configured to receive the financial account information directly from the payer and process the payment.

[10] Note that "mere instructions to implement" the abstract idea of processing a payment from a payer to a payee "on a computer" could be done in far fewer words than are recited in claim 1. For instance, "mere instructions to implement" a method of processing a payment would not require a secure server in addition to the merchant server,

the Patent Office fails to even consider how the claims "as a whole" provide a meaningful limit on the broad concept of processing a payment from a payer to a payee and are, instead, directed to a specific practical application of that broad concept.

B. Additionally, the specific technical features recited in the claims also amount to "significantly more" than "a mere instruction to apply" the abstract idea of *processing a payment from a payer to a payee* "on a computer"

Claims directed to a judicial exception under § 101 are nevertheless patent eligible if the claims recite "significantly more" than an instruction to apply the judicial exception. "Courts have held computer-implemented processes not to be significantly more than an abstract idea (and thus ineligible) where the claim as a whole amounts to nothing more than generic computer functions merely used to implement an abstract idea, such as an idea that could be done by a human analog (i.e., by hand or by merely thinking). On the other hand, courts have held computer-implemented processes to be significantly more than an abstract idea (and thus patent eligible), where generic computer components are able in combination to perform functions that are not merely generic."[11]

In *DDR Holdings*, for example, the Federal Circuit held that claims were patent eligible "because they do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks."[12] There, the specific issue was that, "upon the click of an advertisement for a third-party product displayed on a host's website, the host website would lose that visitor as he or she is "transported to the third party's website." To solve that problem, the claims were directed to "an automatically-generated hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website related to the clicked advertisement. In this way, rather than

---

nor the establishment of a communications link between the secure server and the payer, let alone generating an electronic data token representing financial account information received from the payer (and transmitting the electronic data token for transmittal to the merchant server). Instead, the merchant server could simply receive the financial account information directly from the payer and process the payment.

[11] MPEP 2106.05(d)(II) citing *DDR Holdings, LLC v. Hotels.com, LP*, 773 F. 3d 1245, 1257-59 (2014)

[12] *DDR*, 773 F.3d at 1257.

instantly losing visitors to the third-party's website, the host website can instead send its visitors to a web page on the outsource provider's server that 1) incorporates 'look and feel' elements from the host website, and 2) provides visitors with the opportunity to purchase products from the third-party merchant without actually entering that merchant's website."[13]

As stated in the MPEP, claims that "amount to more than merely instructing that the abstract idea should be applied on the Internet," [14] for example claims that "specify ***how*** interactions with the Internet are manipulated to yield a desired result",[15] may provide a sufficient inventive concept to render claims patent eligible.

Like the claims at issue in *DDR*, the pending claims "do not merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet." Instead, like the claims at issue in *DDR*, the pending claims recite specific technical features that "specify how interactions with the Internet are manipulated to yield a desired result". Like the claims at issue in *DDR*, the pending claims "overcome a problem specifically arising in the realm of computer networks" – namely that, to process a payment online using conventional technology, merchants need to receive sensitive financial account information. Finally, like the claims at issue in *DDR*, the claimed solution to that problem is rooted in computer technology – specifically, a secure server that, in response to an electronically-generated payment transaction instruction from a merchant server, establishes a communications link with a payer to receive financial account information and provides an electronic data token representing that financial account information to a merchant server (without providing the financial account information to the merchant server and without providing the electronic data token to the payer). Accordingly, because the electronic data token is non-sensitive, the claimed secure server allows the merchant to conduct a transaction without the need to receive, store, and safeguard sensitive financial information of the purchaser.[16]

---

[13] *Id.* at 1257-1258(internal footnote omitted)
[14] MPEP 2106.05(f)
[15] MPEP 2106.05(d)(emphasis in original) citing *DDR*, 773 F.3d at 1258
[16] Note that, in embodiments where the communications link between the secure server and the payer "is a widget or window within a website provided by the merchant server" (dependent claims 9 and 24), the claimed solution is even more like the solution in *DDR* in that it is "an automatically-generated hybrid web page that combines visual 'look and feel' elements" from the merchant server website and functionality to provide financial account

In Step 2B, the pending Office Action again simply concludes that the claims "amount to mere instructions to implement" the abstract idea of processing a payment from a payer to a payee "on a computer." Again, the Patent Office fails to consider the claims "as a whole" and even contemplate whether the specific processing steps "perform functions that are not merely generic."

Accordingly, the Applicant respectfully submits that the pending claims are patent eligible subject matter under § 101.

V. NEW CLAIMS

As described above, claims 1-15 are directed to a method performed by a secure server in a merchant server. Claims 16-25 are directed to the secure server. New dependent apparatus claims 26-30 are added that recite the features of dependent method claims 11-16. The Applicant respectfully submits that new claims 26-30 are allowable for at least the reasons described above.

Additionally, new claims 31-45 are added, which are directed to a method, performed by the merchant server in communication with the secure server, to enroll the payer by:

- receiving enrollment data identifying a payer;
- generating an electronic instruction for a secure server that includes at least one data element associated with the payer, the electronic instruction requesting the establishment of a communications link between the secure server and the payer for the secure server to receive financial account information provided by the payer;
- outputting the electronic instruction to a communications network for transmittal to the secure server;
- receiving, from the secure server, an electronic data token representing financial account information received by the secure server via the communications link, wherein the merchant server does not receive the financial account information represented by the electronic data token and the secure server does not provide the electronic data token to the payer;

information to the third-party secure server. In those embodiments, the merchant server sends its visitors to a website "that 1) incorporates 'look and feel' elements from the [merchant server] website, and 2) provides visitors with the opportunity" to submit sensitive financial account information to the third-party secure server "without actually entering" that secure server's website.

- storing the electronic data token in association with the enrollment data identifying the payer; and
- processing a payment from the payer by electronically generating a payment transaction instruction that includes a representation of the electronic data token and instructs a payment processing system having access to the financial account information represented by the electronic data token.

Finally, new claim 46 is added, which is directed to the merchant server. The Applicant respectfully submits that new claims 31-46 are allowable for at least the reasons described above.

VI. CONCLUSION

In view of the above amendment, the Applicant believes the pending application is in condition for allowance.

Please charge any shortage or credit any overpayment of fees to BLANK ROME LLP, Deposit Account No. 23-2185, under Order No. 124452.00122. In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition does not accompany this Amendment or is insufficient to render this Amendment timely, the Applicant hereby petitions under 37 C.F.R. §1.136(a) for an extension of time for as many months as required to render this submission timely. Any fee due is authorized above.

Dated: September 9, 2021

Respectfully submitted,

By: /Michael C. Greenbaum/
Michael C. Greenbaum
Registration No.: 28,419
BLANK ROME LLP
Correspondence Customer Number: 27557
Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	16535424
Filing Date:	08-Aug-2019
Title of Invention:	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System
First Named Inventor/Applicant Name:	Robert Evan POLLIN
Filer:	Michael C. Greenbaum/Crystal Corsey
Attorney Docket Number:	124452.00122

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	740	740
Miscellaneous:				
			Total in USD ($)	**740**

Electronic Acknowledgement Receipt

EFS ID:	43719040
Application Number:	16535424
International Application Number:	
Confirmation Number:	2047
Title of Invention:	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System
First Named Inventor/Applicant Name:	Robert Evan POLLIN
Customer Number:	27557
Filer:	Michael C. Greenbaum/Crystal Corsey
Filer Authorized By:	Michael C. Greenbaum
Attorney Docket Number:	124452.00122
Receipt Date:	09-SEP-2021
Filing Date:	08-AUG-2019
Time Stamp:	11:20:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$740
RAM confirmation Number	E202199B21102047
Deposit Account	022555
Authorized User	Crystal Corsey

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		20210909_ResponseNFOA031721.pdf	247265 a8c265e6f103200fb86a477f45bcefac69749e85	yes	23

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	14
Applicant Arguments/Remarks Made in an Amendment	15	23

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	38451 ba52f240beb1617ca37ceadee7067abb20265e43	no	2

Warnings:

Information:

Total Files Size (in bytes):	285716

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

Courtesy Reminder for
Application Serial No: 16/535,424

Attorney Docket No: 124452.00122
Customer Number: 27557
Date of Electronic Notification: 03/17/2021

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:
WashingtonDocketing@blankrome.com

To view your correspondence online or update your email addresses, please visit us anytime at **https://ppair-my.uspto.gov/pair/PrivatePair.**
If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122	2047

27557 7590 03/17/2021

BLANK ROME LLP
1825 EYE STREET NW
WASHINGTON, DC 20006-5403

EXAMINER	
MACCAGNO, PIERRE L	

ART UNIT	PAPER NUMBER
3696	

NOTIFICATION DATE	DELIVERY MODE
03/17/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

WashingtonDocketing@blankrome.com

Office Action Summary	Application No. 16/535,424	Applicant(s) POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3696	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 8-8-2019.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-25 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-25 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 8-8-2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☑ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Status of Claims

1. This action is a non-final rejection.
2. Claims 1-25 are rejected under **35 USC § 101**

Priority

Acknowledgement is made of Applicant's claim for a foreign priority date of 6-5-2012.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 8-8-2019, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims **[1-25]** are not patent eligible because the claimed invention is directed to an abstract idea without significantly more.

Analysis

First, claims are directed to one or more of the following statutory categories: a process, a machine, a manufacture, and a composition of matter. Regarding claims **1-25**, the claims recite an abstract idea of processing a payment from a payer to a payee.

Independent Claims 1, 14 and 25 are rejected under 35 U.S.C 101 based on the following analysis.

-Step 1 (Does the claim fall within a statutory category? YES): claims 1, 14 and 25 recite a method, system and non-transitory computer readable storage medium respectively for processing a payment from a payer to a payee.

-Step 2019 PEG 2A Prong One (Does the claim fall within at least one of the groupings of abstract ideas?: YES): The claimed invention "includes at least one data element associated with the payer "; "specifies the amount of the payment from the payer to the payee"; "obtaining the financial account information from the payer"; "obtaining the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer"and "forwarding at least a portion of the amount of the payment to the payee"; falls under the grouping of certain methods of organizing human activity under fundamental economic practices as it recites processing a payment from a payer to a payee. (refer to MPEP 2106.04(a)(2)). Accordingly this claim recites an abstract idea.

-Step 2019 PEG 2A Prong Two (Are there additional elements in the claim that imposes a meaningful limit on the abstract idea? NO). Claims 1, 14 & 25 recite: "a first computing system"; "a second computing system "; "specifies a communications link for the second computing system to obtain financial account information from the payer"; "generating an electronic data token representing the financial account information obtained from the payer"; and "outputting the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer". In addition claim 14 recites: "one or more processors"; and memory storing instructions "; and in addition claim 25 recites "A non-transitory computer readable storage medium storing instructions that, when executed by a processor"; amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea. (refer to MPEP 2106.05(f))

Claims 1, 14 and 25 also recite: "receiving a second payment transaction instruction from the first computing system"; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering. (refer to MPEP 2106.05(g). Accordingly, the claim as a whole does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea.

-Step 2019 PEG 2B (Does the additional elements of the claim provide an inventive concept?: NO. As discussed previously with respect to Step 2A Prong Two, Claims 1, 14

& 25 recite: “a first computing system”; “a second computing system “; “specifies a communications link for the second computing system to obtain financial account information from the payer“; “generating an electronic data token representing the financial account information obtained from the payer“; and “outputting the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer“. In addition claim 14 recites: “one or more processors”; and memory storing instructions “; and in addition claim 25 recites “A non-transitory computer readable storage medium storing instructions that, when executed by a processor“; amount to mere instructions to implement an abstract idea on a computer, or merely use a computer as a tool to implement the abstract idea. (refer to MPEP 2106.05(f))

Claims 1, 14 and 25 also recite: “receiving a second payment transaction instruction from the first computing system”; that amount to additional insignificant extra solution activities to the judicial exception specific to data gathering. (refer to MPEP 2106.05(g). Under Step 2B further analysis under well-understood routine conventional (WURC) is required which includes consideration of the four options per the Berkheimer memo. Using WURC option 2 “receiving data”; “sending data” ; “transmitting data”; “selecting data”; “presenting data”; or “gathering data” can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Accordingly, the claim does not provide an inventive concept (significantly more than the abstract idea) and hence the claim is ineligible.

Claims 2-13, dependent on claim 1 and claims 15-24 dependent on claim 14 are rejected under 35 U.S.C 101 based on similar rationale as claims 1 and 14 respectively. The additionally recited elements in the dependent claims were all individually and collectively examined and found to merely refine and/or further limit the abstract idea(s) of the independent claim(s). They do not add any feature which integrates the judicial exception into a practical application, nor do they amount to significantly more, indicative of an inventive concept which cures the deficiencies of their respective parent independent claim or transforms the nature of the claims into patent-eligible subject matter under 35 USC §101.

Claim 2 dependent on claim 1, and claim 15 dependent on claim 14 merely adds to the abstract idea of claims 1 and 14 respectively. By reciting "specifies the amount of the second payment from the payer to the payee"; and "forwarding the amount of the second payment to the payee"; it adds to the abstract idea of processing a payment from a payer to a payee by specifying the amount of the second payment from the payer to the payee, and forwarding the payment to the payee without adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Claim 2 dependent on claim 1 and claim 15 dependent on claim 14 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the second payment transaction instruction: includes a representation of the electronic data token" and "processing the second payment using the financial account information represented by the electronic data token"; accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f).

Claim 2 dependent on claim 1 and claim 15 dependent on claim 14 merely recite additional steps that amount to no more than insignificant extra-solution activities to the judicial exception. Specifically claims 2 and 15 recite "receiving a second payment transaction instruction from the first computing system". This claim amounts to additional insignificant extra solution activities to the judicial exception specific to data gathering, which is a form of insignificant extra-solution activity (refer to MPEP 2016.05 (g). Such limitation does not integrate the abstract idea into a practical application. Further analysis under WURC option 2 "receiving data"; "sending data" ; "transmitting data"; "selecting data"; "presenting data"; or "gathering data" can be said to be recognized by the courts as simply WURC (see MPEP 2106.05 (d)(II)). Such limitation does not amount to significantly more than an abstract idea and hence the claim is ineligible.

Claim 3 dependent on claim 1 and claim 16 dependent on claim 14 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used by the first computing system to obtain enrollment data from the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 4 dependent on claim 1 amount to mere instructions to apply the abstract idea of claim 1 using a generic computer, by reciting "wherein the communications link is at least one of a telephone number to enable the second computing system to communicate with the payer and obtain the financial account information or a transfer from an existing telephone call with the payer to a telephone system that receives the financial account information from the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 5 dependent on claim 1 and claim 17 dependent on claim 14 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the communication link is a connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 6 dependent on claim 5 and claim 18 dependent on claim 17 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the connection is a widget or window within a website provided by the first computing system". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 7 dependent on claim 5 and claim 19 dependent on claim 17 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the connection provides access to the second computing system using a static or dynamic universal resource locator (URL)". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 8 dependent on claim 1 and claim 20 dependent on claim 14 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the communications link used to obtain the financial account information from the payer is asynchronous with a communications link used by the first computing system to obtain enrollment data from the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 9 dependent on claim 8 and claim 21 dependent on claim 20 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the payment transaction instruction for the second computing system to obtain the financial account information from the payer includes data sufficient for the second computing system to authenticate the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 10 dependent on claim 9 and claim 22 dependent on claim 21 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the first computing system defines a period of persistence for the second computing system to obtain the financial account information from the payer". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 11 dependent on claim 1 and claim 23 dependent on claim 14 amount to mere instructions to apply the abstract idea of claims 1 and 14 respectively using a generic computer, by reciting "wherein the payment transaction instruction comprises contact information for the payer to enable the second computing system to transmit instructions to the payer for communicating the financial account information to the second computing system". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 12 dependent on claim 11 amounts to mere instructions to apply the abstract idea of claim 1 using a generic computer, by reciting "wherein the contact information comprises one of an email address or a telephone number whereby the second computing system sends a link for a data entry connection to the payer via one of email and text". Accordingly the claim is rejected under 35 U.S.C. 101 based on MPEP 2106.05(f)

Claim 13 dependent on claim 1, and claim 24 dependent on claim 14 merely adds to the abstract idea of claims 1 and 14 respectively. By reciting "wherein the financial account information includes at least one of a credit card number or bank account number"; it adds to the abstract idea of processing a payment from a payer to a payee by specifying that the financial account information includes at least a credit card number or bank account number without adding any additional elements that impose a meaningful limit on the abstract idea or any additional elements in the claim providing an inventive concept. As a result it is rejected under 35 U.S.C. 101 based on MPEP 2106.04(a)(2).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE L MACCAGNO whose telephone number is (571)270-5408. The examiner can normally be reached on M-F 8:00 to 5:00.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, supervisory patent examiner, Boveja Namrata can be reached at 571-272-8105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PIERRE L MACCAGNO/
Examiner, Art Unit 3696

/Robert R Niquette/
Primary Examiner, Art Unit 3696

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3696	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20130198080-A1	08-2013	Anderson; Lisa	G06Q20/26	705/44
*	B	US-20120259782-A1	10-2012	Hammad; Ayman	G06Q20/382	705/44
*	C	US-20120030066-A1	02-2012	Stringfellow; Westley	G06Q20/12	705/26.41
*	D	US-20120023567-A1	01-2012	Hammad; Ayman	G06Q20/4016	726/9
*	E	US-20110184853-A1	07-2011	Mark; Timothy James	G06Q20/3221	705/39
*	F	US-20110078244-A1	03-2011	Minter; David D.	G06Q30/02	709/204
*	G	US-20110029436-A1	02-2011	Norvell; Joel	G06Q30/02	705/67
*	H	US-20090132351-A1	05-2009	Gibson; Garry H.	G06Q20/02	705/12
*	I	US-20090048953-A1	02-2009	Hazel; Patrick	G07F7/1008	705/35
*	J	US-20050197962-A1	09-2005	Critchfield, Steve Taylor	G06Q50/26	705/53
*	K	US-20040143550-A1	07-2004	Creamer, Thomas E.	G06Q20/105	705/41
*	L	US-20020107791-A1	08-2002	Nobrega, Ryan J.	G06Q20/327	705/39
*	M	US-20020087704-A1	07-2002	Chesnais, Pascal	H04L69/329	709/228

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.	
	Examiner PIERRE L MACCAGNO	Art Unit 3696	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20010056402-A1	12-2001	Ahuja, Arun	G06Q20/1085	705/43
*	B	US-7801825-B2	09-2010	Kranzley; Arthur D.	G06Q20/04	705/67
*	C	US-20140074695-A1	03-2014	BARKAN; Mordhay	G06Q20/3674	705/39
*	D	US-20110029416-A1	02-2011	Greenspan; Aaron J.	G06Q20/10	705/30
*	E	US-20020165821-A1	11-2002	Tree, Ian David	G06Q20/04	705/39
*	F	US-20070011093-A1	01-2007	Tree; Ian David	G06Q20/10	705/40
*	G	US-20090063353-A1	03-2009	Viidu; Siim	G06Q20/16	705/75
*	H	US-7680736-B2	03-2010	Jarman; Jonathan S.	G06Q20/202	705/41
*	I	US-20110161233-A1	06-2011	Tieken; Craig A.	G06Q20/4014	705/71
*	J	US-20080083826-A1	04-2008	Henry; James M.	G06Q20/10	235/379
*	K	US-20090240594-A1	09-2009	Kerner; Robert	G06Q30/0601	705/26.1
*	L	US-7120609-B1	10-2006	Kerkdijk; Hendrikus	G06Q20/02	705/78
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Robert E. Pollin
Art Unit	
Examiner Name	
Attorney Docket Number	124452-00122

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7801825		2010-09-21	Kranzley et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090132351	A1	2009-05-21	Gibson	
	2	20010056402	A1	2001-12-27	Ahuja et al.	
	3	20020087704	A1	2002-07-04	Chesnais et al.	
	4	20040143550	A1	2004-07-22	Creamer et al.	
	5	20050197962	A1	2005-09-08	Critchfield et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

	6	20070250920	A1	2007-10-25	Lindsay	
	7	20110029436	A1	2011-02-03	Norvell et al.	
	8	20110078244	A1	2011-03-31	Minter et al.	
	9	20120030066	A1	2012-02-02	Stringfellow et al.	
	10	20020107791	A1	2002-08-08	Nobrega et al.	
	11	20110184853	A1	2011-07-28	Mark et al.	
	12	20120023567	A1	2012-01-26	Hammad	
	13	20120259782	A1	2012-10-11	Hammad	
	14	20130198080	A1	2013-08-01	Anderson et al.	
	15	20090048953	A1	2009-02-19	Hazel	
	16	20060235796	A1	2006-10-19	Johnson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Robert E. Pollin
	Art Unit	
	Examiner Name	
	Attorney Docket Number	124452-00122

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	
Name/Print	Michael C. Greenbaum	Registration Number	28419

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date
15/408,185	January 17, 2017

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 27557

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Autoscribe Corporation

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	Robert E Pollin	Date (Optional)	5/21/2019
Name	Robert E. Pollin		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Docket No.: 124452-00122
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert E. Pollin et al.

Application No.: Not Yet Assigned | Confirmation No.: Not Yet Assigned

Filed: Concurrently Herewith | Art Unit: Not Yet Assigned

For: Processing A Payment, By A Second Computing System, From A Payer To A Payee Operating A First Computing System | Examiner: Not Yet Assigned

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement accompanies the new patent application submitted herewith.

Copies of the references on the PTO/SB/08 are not provided.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed

to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to the patentability as defined in 37 C.F.R. § 1.56(b).

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98, and the Examiner is respectfully requested to consider the listed references.

The Director is hereby authorized to charge any additional fees which may be required with respect to this communication, or credit any overpayment, to Deposit Account No. 23-2185, under Order No. 124452-00122.

Dated:

Respectfully submitted,

Electronic signature:/Michael C. Greenbaum/
Michael C. Greenbaum
Registration No.: 28,419
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
(202) 772-5800
Attorney for Applicant

PTO/AIA/15 (10-17)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	124452-00122
First Named Inventor	Robert E. Pollin
Title	Processing A Payment By A Second Computing...
Priority Mail Express® Label No.	VIA EFS

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (PTO/SB/17 or equivalent)
2. ☑ **Applicant asserts small entity status.** See 37 CFR 1.27
3. ☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
4. ☑ **Specification** [*Total Pages* 30] Both the claims and abstract must start on a new page. *(See MPEP § 608.01(a) for information on the preferred arrangement)*
5. ☑ **Drawing(s)** (35 U.S.C. 113) [*Total Sheets* 15]
6. **Inventor's Oath or Declaration** [*Total Pages* ____] *(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))*
   a. ☐ Newly executed (original or copy)
   b. ☑ A copy from a prior application (37 CFR 1.63(d))
7. ☑ **Application Data Sheet** ** See note below.* See 37 CFR 1.76 (PTO/AIA/14 or equivalent)
8. **CD-ROM or CD-R** in duplicate, large table, or Computer Program (*Appendix*)
   ☐ Landscape Table on CD
9. **Nucleotide and/or Amino Acid Sequence Submission** (*if applicable, items a. – c. are required*)
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

ACCOMPANYING APPLICATION PAPERS

10. ☐ **Assignment Papers** (cover sheet & document(s)) Name of Assignee ____
11. ☐ **37 CFR 3.73(c) Statement** (*when there is an assignee*) ☑ **Power of Attorney**
12. ☐ **English Translation Document** (*if applicable*)
13. ☑ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
14. ☐ **Preliminary Amendment**
15. ☐ **Return Receipt Postcard** (*MPEP § 503*) (*Should be specifically itemized*)
16. ☐ **Certified Copy of Priority Document(s)** (*if foreign priority is claimed*)
17. ☐ **Nonpublication Request** Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
18. ☐ **Other:** ____

*Note: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 27557 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Michael C. Greenbaum/	Date	August 8, 2019
Name (Print/Type)	Michael C. Greenbaum	Registration No. (Attorney/Agent)	28,419

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	124452.00122
	Application Number	
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Robert	Evan	POLLIN	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Rockville	MD	US

Mailing Address of Inventor:

Address 1	1045 Wintergreen Terrace
Address 2	

City	State/Province	Postal Code	Country
Rockville	MD	20850	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Brian	Edward	DOWNEY	Jr.

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Alexandria	VA	US

Mailing Address of Inventor:

Address 1	6133 Wellington Commons Drive
Address 2	

City	State/Province	Postal Code	Country
Alexandria	VA	22310	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	Sean	Allen	FLEMING	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	124452.00122
	Application Number	
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System	

City	Germantown	State/Province	MD	Country of Residence	US

Mailing Address of Inventor:

Address 1	19959 Dunstable Cir.		
Address 2			
City	Germantown	**State/Province**	MD
Postal Code	20876	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	27557		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System		
Attorney Docket Number	124452.00122	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	15	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	124452.00122
	Application Number	
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System	

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	27557		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	15408185	2017-01-17
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15408185	Continuation of	13679545	2012-11-16	9576279	2017-02-21

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13679545	non provisional of	61655482	2012-06-05
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
13679545	non provisional of	61698574	2012-09-08

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Priority Claimed
			Yes No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Authorization to Permit Access:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	124452.00122
	Application Number	
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System	

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Remove

● Assignee	Legal Representative under 35 U.S.C. 117
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Assignee is an Organization check here. ☒

Organization Name	Autoscribe Corporation

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	124452.00122
	Application Number	
Title of Invention	Processing A Payment By A Second Computing System From A Payer To A Payee Operating A First Computing System	

Mailing Address Information:			
Address 1	9801 Washingtonian Blvd., Ste 200,		
Address 2			
City	Gaitherburg	**State/Province**	MD
Country	US	Postal Code	20878
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Michael C. Greenbaum/			Date (YYYY-MM-DD)	2019-08-08
First Name	Michael	Last Name	Greenbaum	Registration Number	28419

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PROCESSING A PAYMENT, BY A SECOND COMPUTING SYSTEM, FROM A PAYER TO A PAYEE OPERATING A FIRST COMPUTING SYSTEM

[0001] This application is a continuation of co-pending U.S. Appl. No. 15/408,185, filed January 17, 2017, which is a continuation of U.S. Appl. No. 13/679,545, now U.S. Pat. No. 9,576,279, filed November 16, 2012, which claims the benefit of U.S. Prov. Pat. Appl. No. 61/655,482, filed June 5, 2012, and U.S. Prov. Pat. Appl. No. 61/698,574, filed September 8, 2012. The aforementioned patent applications are hereby incorporated by reference in their entirety.

Field of the Invention

[0002] The present invention relates broadly to systems and methods for obtaining and using account information to process financial payments.

Background

[0003] Fraud in credit card and other financial transactions is a major problem, and considerable resources are devoted to securing credit card and other account information provided to merchants by payers. A single breach of security incident can compromise millions of credit card accounts, and such breaches are reported on a regular basis.

[0004] The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

[0005] Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud. Annual PCI compliance audits by an external Qualified Security Assessor (QSA) are required for organizations handling large volumes of transactions. The security and organizational measures required to comply with the PCI standards, and the cost of the annual audits, are borne by the individual organization. Underlying software applications may require substantial modifications to achieve compliance, and significant changes in organizational structure and operating procedures may also

be required. Thus, the time, effort, and cost required for merchants and processors to obtain PCI certification to receive and use credit card data are substantial.

[0006] In one approach to managing these costs, credit card processing organizations have used tokenization to provide a link to credit card data for purposes of storage and retrieval. Tokenization is the process of replacing some piece of sensitive data with a value that is not considered sensitive outside the environment where it is stored and used. The token is a symbolic representation of a financial instrument or instruction that is only meaningful to participants in the processing cycle, and safeguards the permissible use of and access to the financial instrument to authorized users. In the payments industry, tokenization has become a popular means of bolstering the security of electronic transactions while minimizing the complexity of compliance with industry standards and best practices.

[0007] In the PCI context, tokens are used to reference cardholder data that is stored in a separate database, application or off-site secure facility that is PCI compliant to the appropriate level. Therefore, the token, which is non-sensitive data, can be stored and used in a wide range of systems in the organization, without bringing those systems within the scope of a higher-level PCI audit and more stringent compliance requirements.

[0008] However, there are limits in functionality of existing tokenization methods. There is a need for improvement in conventional approaches to obtaining and using account information to process financial payments.

Summary of the Invention

[0009] It is to be understood that both the following summary and the detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed. Neither the summary nor the description that follows is intended to define or limit the scope of the invention to the particular features mentioned in the summary or in the description.

[0010] In an example embodiment, an authenticated customer (payer) enrollment session is established, and a last stage of the enrollment session is completed via a communications link such as a telephone or Internet link. The enrollment session is initiated, for example, by a merchant or collector who has obtained at least an initial identification of the customer (also sometimes referred to as the payer). In an embodiment, an initial portion of the enrollment session is completed on

the merchant's server, or a third-party server providing services to the merchant, with data entered by a customer service agent who receives information over a telephone, by a customer over a network such as the Internet, or using an initial data file received from another source, such as a file listing customer identification information for debt collection purposes. A second portion of the enrollment session is then completed on a secure server that may be different from the merchant's server. In a preferred embodiment, financial account information used to make one or more payments is submitted to the secure server while other less sensitive data elements such as the customer's name and address are submitted to the merchant's regular server. For convenience the server that stores the sensitive financial account information will be referred to herein as the "secure" server, but this naming convention should not be interpreted to suggest that the merchant's regular server cannot have security features or be highly secure in its own right. In some embodiments, the merchant's server and secure server may operate in the same location or may be the same hardware using a separated volume or partition, or memory section. However, in other embodiments particular advantages are realized through logical and/or physical separation of the merchant's server and the secure server.

[0011] The secure server, in a preferred embodiment, stores the financial account information received from the customer (either in the secure server or in a separate secure storage location) and provides a token to the merchant's server. Financial account information may include, for example, credit card numbers and security codes, bank routing and account numbers, or other financial account identifiers. While certain advantages can be realized by storing financial account information on the secure server, storage of data on the secure server is not limited to such information; the secure server may receive and store information other than financial account information, to the extent the merchant wishes to store such additional information on the secure server rather than on the merchant's server. The token is an index to the stored financial account information for that customer that is stored by the merchant (or a server or service controlled by the merchant or merchant's agent) in connection with the customer record and is used to identify the customer account to be debited to process a payment authorized by the customer.

[0012] To process a payment from the customer, the merchant submits information specifying the amount of the payment to the secure server. The operator of the secure server then processes the payment using the financial account pointed to by the token and makes the proceeds available to the merchant. By retaining the token corresponding to the customer account to be debited, the

merchant retains control of the customer's enrollment information and the ability to process payments whenever authorized (using financial account information provided by the customer) but does not hold the underlying financial account information or have security responsibility for that information.

Brief Description of the Drawings

[0013] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate various exemplary embodiments of the present invention and, together with the description, further serve to explain various principles and to enable a person skilled in the pertinent art to make and use the invention.

[0014] Figure 1 is a block schematic diagram of an example computing system that can be used to implement functions described herein;

[0015] Figure 2 is a block diagram illustrating connections of servers and systems in an example embodiment;

[0016] Figure 3 is a flow chart showing a method of registering customer financial information and processing payments in an example embodiment;

[0017] Figures 4a through 4l together comprise a flow chart showing a further example embodiment of the process disclosed herein.

Detailed Description of the Preferred Embodiments

[0018] The present invention will be described in terms of one or more examples, with reference to the accompanying drawings.

[0019] The present invention will also be explained in terms of exemplary embodiments. This specification discloses one or more embodiments that incorporate the features of this invention. The disclosure herein will provide examples of embodiments, including examples of data analysis from which those skilled in the art will appreciate various novel approaches and features developed by the inventors. These various novel approaches and features, as they may appear herein, may be used individually, or in combination with each other as desired.

[0020] In particular, the embodiment(s) described, and references in the specification to "one embodiment," "an embodiment," "an example embodiment," etc., indicate that the embodiment(s)

described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, persons skilled in the art may implement such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0021] Embodiments of the invention may be implemented in hardware, firmware, software, cloud computing, or any combination thereof. Embodiments of the invention may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g. a computing device). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); hardware memory in handheld computers, PDAs, mobile telephones, and other portable devices; magnetic disk storage media; optical storage media; thumb drives and other flash memory devices; electrical, optical, acoustical, or other forms of propagated signals (e.g. carrier waves, infrared signals, digital signals, analog signals, etc.), Internet cloud storage, and others. Further, firmware, software, routines, instructions, may be described herein as performing certain actions. However, it should be appreciated that such descriptions are merely for convenience and that such actions in fact result from computing devices, processors, controllers or other devices executing the firmware, software, routines, instructions, etc.

[0022] Figure 1 is a block schematic diagram of an example embodiment of a computing system that can be used to perform the functions disclosed herein in both server and end user applications. The example embodiment shows a general-purpose computer system 700, such as a PC system. In particular, the methods disclosed herein can be implemented in hardware, or implemented as a combination of software and hardware. Consequently, desired features of the invention may be implemented in the environment of a computer system or other processing system. The example computer system 700 includes one or more processors, such as processor 704. Processor 704 can be a special purpose or a general-purpose digital processor. The processor 704 is connected to one or more communication infrastructures 706 (for example, a bus or network). Various software implementations are described in terms of this exemplary computer

system. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures.

[0023] Computer system 700 also includes a main memory 705, preferably random access memory (RAM), and may also include a secondary memory 710. The secondary memory 710 may include, for example, a hard disk drive 712, and/or a RAID array 716, and/or a removable storage drive 714, representing an optical disk drive, solid state memory, USB port for a thumb drive, PC card slot, SD card slot for a flash memory, communications conduit to a cloud storage server or service, or other storage device. Secondary memory 710 may also include information storage in another location, but accessible through a network interface, such as storage on a separate computing system or a cloud. The removable storage drive 714 reads from and/or writes to a removable storage unit 718 in a well-known manner. Removable storage unit 718, for example, may be a magnetic drive, optical disk, thumb drive, flash memory device, etc. As will be appreciated, the removable storage unit 718 includes a computer usable storage medium having stored therein computer software and/or data.

[0024] In alternative implementations, secondary memory 710 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 700. Such means may include, for example, a removable storage unit 722 and an interface 720. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 722 and interfaces 720 which allow software and data to be transferred from the removable storage unit 722 to computer system 700.

[0025] Computer system 700 may also include a communications interface 724. Communications interface 724 allows software and data to be transferred between computer system 700 and external devices. Examples of communications interface 724 may include a modem, a network interface (such as an Ethernet interface), a communications port, a wireless network communications device such as an IEEE 802.11x wireless Ethernet device, 3G or 4G cellular data connection, a PC slot and card, cloud or network storage, etc. Software and data transferred via communications interface 724 are in the form of signals 728 which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface 724. These signals 728 are provided to communications interface 724 via a

communications path 726. Communications path 726 carries signals 728 and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other present or future available communications channels.

[0026] The terms "computer program medium" and "computer usable medium" are used herein to generally refer to all available types of digital media, for example, removable storage drive 714, a hard disk installed in hard disk drive 712, and signals 728. These computer program products are means for providing software to computer system 700.

[0027] Computer programs (also called computer control logic) are stored in main memory 708 and/or secondary memory 710. Computer programs may also be received via communications interface 724. Such computer programs, when executed by the processor 704, enable the computer system 700 to implement the present invention as discussed herein. In particular, the computer programs, when executed, enable the processor 704 to implement the processes of the present invention. Where the invention is implemented using software, the software may be provided as a computer program product on media or transmitted digitally via one of the network connections available to computer system 700, and loaded into computer system 700, for example on raid array 716, removable storage drive 714, hard drive 712 or communications interface 724. The conventional, general-purpose computer systems described herein are customized to form a special purpose, inventive device by the installation of novel software that implements and enables novel methods. This software and the methods employed will now be described in more detail. The scope of the present invention is not limited to the specific examples provided here, but those skilled in the art will gain an understanding of the full scope of the invention through illustrations provided in a series of example embodiments.

[0028] Referring to Figure 2, in one example embodiment, an inventive system and method make functions available to merchants (and to third-party service providers to merchants) in an Application Programming Interface (API). A hosted system on a secure server 202 provides Financial Account Registration functions and Token Retrieval functions that can be accessed by merchants and others operating websites, for example using merchant server 204, to process payment transactions. Using the methods disclosed herein, in preferred embodiments merchants are able to process such transactions without transmitting, processing or storing Financial Account data. This reduces the potential liability of the merchants for data loss, and avoids placing their

customer tracking and payment processing systems (such as merchant server 204) within the scope of the present Payment Card Industry Data Security Standard (PCI-DSS), thus reducing compliance costs, development costs, and accelerating time-to-market.

[0029] The server that stores the sensitive financial account information will be referred to herein as the "secure server," but this naming convention should not be interpreted to suggest that merchant server 204 cannot also have security features, or otherwise be highly secure in its own right. Further, while server 204 is described in these examples as a "merchant" server for convenience, the systems and processes disclosed herein are not limited to merchants, but are applicable to any operation that needs to process payments. Thus, merchant server 204 may serve merchants, debt collectors, non-profit organizations, political campaigns, service providers of any type, processors serving merchants or sub-merchants, and in general any individual or organization of any type that wishes to process payments from one or more individuals. Further, merchant server 204 may be operated by a third-party service provider to one or more merchants or other entities that wish to process payments using the methods disclosed herein.

[0030] Merchant server 204 and secure server 202 are connected by a communications network, such as the Internet, and can also be accessed by computer systems at one or more customer locations represented as 206, 208, and 210. A telephone interactive voice response interface 212 may be connected to secure server 202 and to the telephone network, allowing customer location 210 to provide information to the secure server via telephone, by speech recognition or tone entry. Similarly, a variety of other known communications networks, represented by the example of SMS data network 214, may be connected to secure server 202 to provide a link to customer equipment for receipt of payment information. The inventors anticipate that any available communications network, whether currently available or newly developed, may be used by the customers to provide financial account information in a secure manner to secure server 202.

[0031] The secure server 202, merchant server 204, and computers at customer locations 206, 208, and 210 may be, for example, general purpose computers such as the computer hardware described with reference to Figure 1. Merchant server 204 and secure server 202 are provided with custom financial information registration software performing one or more functions described in example embodiments herein. The secure server 202 and merchant server 204 are

also provided with Internet web server software allowing interactive exchange of information with customer sites 206, 208 and 210 via the World Wide Web. Computer equipment at customer sites 206, 208 and 210 are preferably provided with standard web browser software to facilitate interaction with secure server 202 and merchant server 204 as described in the example embodiments herein. For simplicity, servers 202 and 204 are illustrated in the drawings as single hardware units, but those skilled in the art will appreciate that the invention is not limited to any particular hardware configuration; thus, any desired server configuration can be used to implement the methods disclosed herein, including (as non-limiting examples) multiprocessor, multiple, grouped, parallel, distributed, replicated, and mirrored server configurations.

[0032] The financial account registration and token retrieval functions provided in the API can be implemented, in a first example, within the merchant's website hosted on merchant server 204, in a "widget" or frame, using either static or dynamic URL access to secure server 202 (the hosted system that maintains the financial data). Secure server 202 returns a token or other account identifier constituting a symbolic representation of the financial account information to merchant server 204 after the financial account information has been registered at secure server 202. Thereafter, merchant server 204 may use the token to process further payment transactions authorized by the end user or customer at sites 206, 208, 210 in their interaction with the merchant. Merchant server 204 may store customer identification information, purchase history, and other data that does not include financial account information such as credit card information, without being subject to PCI compliance requirements.

[0033] In an embodiment, an authenticated customer enrollment session is established, and a last stage of the enrollment session is completed via a communications link such as telephone link 212 or Internet link 216. The enrollment session is initiated by a merchant or collector who has obtained at least an initial identification of the customer. In an embodiment, an initial portion of the enrollment session is completed on the merchant's server, with data entry by a customer service agent who receives information over a telephone, by input from the customer over a network such as the Internet, or using an initial data file received from another source, such as a merchant's customer information file.

[0034] A second portion of the enrollment session is then completed on secure server 202. In a preferred embodiment, financial account information used to make one or more payments is

submitted to secure server 202 while other data elements such as the customer's name and address are submitted to merchant server 204. Secure server 202, in a preferred embodiment, stores the financial account information received from the customer (for example from sites 206, 208, or 210) and provides a token to merchant server 204. Financial account information may include, for example, credit card numbers and security codes, bank routing and account numbers, or other financial account identifiers. While certain advantages can be realized by storing financial account information on secure server 202, storage of data on secure server 202 is not limited to such information; secure server 202 may receive and store information other than financial account information, to the extent the merchant wishes to store such additional information on secure server 202 rather than on the merchant server 204. The token is an index to the stored financial account information for that customer, and is stored by the merchant in connection with the customer record, then used by the merchant to identify the customer account to be debited to process a payment authorized by the customer.

[0035] Figure 3 is a flow chart showing an example embodiment of a general method and process for enrolling a payer in an electronic system and then making a payment based on the enrollment. The method starts with step 302, in which enrollment data identifying a payer is stored in a first computing system. The first computing system may be, for example, the merchant server 204 shown in Figure 2. The first computing system may be operated by a merchant, bill collector, or other individual or organization that will be the payee for anticipated payment transactions. As an example, this step can be accomplished by taking information from the payer over the telephone and entering it into merchant server 204, or by the payer entering their identifying information on an Internet website generated by merchant server 204 and operated by the payee or an agent of the payee.

[0036] Next, in step 304, the first computing system (for example, the merchant server 204) generates an electronic instruction to a second computing system, such as secure server 202, to obtain financial account information from the payer. The desired financial account information is distinguished, in this example, from identifying information in that financial account information refers to specific data used to process a payment, such as a credit card number, security code, and expiration date used to charge a credit card account, or the bank account and routing numbers used to process Automated Clearing House (ACH) transactions. The second computing system, in this example secure server 202, may typically be set up to provide a higher level of security than the

merchant server in order to protect the sensitive financial account information that will be stored there, as such information could be used to perpetrate a fraud in case of a security breach. The instruction to the secure server 202 to obtain financial account information may also optionally include information specifying one or more available communications links to be used to obtain this financial account information. For example, as shown in Figure 2, the World Wide Web, computers and mobile devices having access to email, text, SMS messaging, or other data networks, and voice or tone-responsive telephone connections may all be used to obtain the financial account information.

[0037] In step 306, this instruction is transmitted to the second computing system, which in this example is the secure server 202 of Figure 2, for action.

[0038] In step 308, the second computing system communicates with the payer, through any of the communications channels described herein or any other available communications channel. The communications channel to be used may be determined by pre-programmed preferences or by the instruction from the merchant server, as appropriate to the situation. During this communication, the payer is preferably able to provide the sensitive financial account information to the second computing system without this information being visible or audible to personnel employed by the operator of the first computing system.

[0039] In step 310, the financial account information is stored in the second computing system and a token is generated for the referring payee (e.g. the merchant or operator of the merchant server). The token is a pointer that allows the payee to reference the financial account information of that payer without possessing the actual financial account information.

[0040] In step 312, the first computing system receives the token from the second computing system in response to its instruction to obtain financial account information for the payer. The token is stored in the first computing system in association with the electronic enrollment data for the payer. This completes the registration of the payer so as to enable one or more intended payments to the payee using the stored financial account information.

[0041] Next, in step 314, at any time after registration is complete, the payee can process an authorized payment from the payer by electronically generating a payment transaction instruction in the first computing system, including a representation of the token, and electronically transmitting the payment transaction instruction to a computing system other than the first

computing system having access to said financial account information. For example, the instruction may be transmitted to the second computing system, e.g. the secure server 202. However, those skilled in the art will appreciate that computing processes may be divided between computers in a network in any desired manner, and that any number of computers may be used to perform a set of processing steps as is known in the art. Therefore, in this example the inventors have described the process in terms of a relatively simple exchange of data and instructions between two servers, but anticipate that in practice, these functions may be performed in some cases by a single computing system, and in other cases by a plurality of computing devices with the tasks divided between the computers in any desired manner. The second computer system or another computer system that receives the instructions and token (and can access the financial account information based on the token) processes the payment as requested, without the first computing system having any direct access to the payer's financial account information represented by the token.

[0042] In an example embodiment, to process a payment from the customer, merchant server 204 submits the token corresponding to the customer account to be debited and information specifying the amount of the payment to the secure server 202. The operator of the secure server 202 then processes the payment using the financial account pointed to by the token, and makes the proceeds available to the merchant. In this way, the merchant retains control of the customer's enrollment information and the ability to process payments whenever authorized, using financial account information provided by the customer, but does not hold the underlying financial account information or have security responsibility for that information.

[0043] In an embodiment, the enrollment session described with reference to the flow chart of Figure 3 is established under the control of merchant server 204 and may optionally have a defined period of persistence, during which the second portion of the enrollment (submission of financial account information to the second computing system) is completed through secure server 202. The session may be set to expire after a specified time, if the second portion of the enrollment, e.g. the submission of financial account information to be linked with the enrollment, is not completed within that period.

[0044] The communications link established between the end user at locations 206, 208, 210 and the secure server 202 to complete the enrollment process may be either synchronous with the

data link used to enter information into the merchant's server, or may be asynchronous. As non-limiting examples of communications channels that can be used for storing information on the secure server, telephone link 212, Internet link 216, and other available links such as SMS link 214 may be used to obtain the information.

[0045] Telephone. The customer may be transferred to, or invited to call, or may receive an automated call after having provided his/her telephone number, from an interactive voice response (IVR) system associated with the secure server operating through telephone interface 212. In this manner the customer may key in or speak the account number, preferably without any merchant representatives present on the call (although a three-way call can also be implemented if desired), and thus store this information in secure server 202.

[0046] Internet. Merchant server 204 may provide the customer at site 206, 208 or 210 with a widget or redirected URL that provides an online window for direct, preferably secure communication with the secure server 202 for entry of financial account information. If desired, the widget or window may be designed to appear as part of the merchant's data entry screen transmitted to the customer's browser from merchant server 204, so that the process of registering with data stored on two separate servers is seamless from the viewpoint of the customer. In another embodiment, the customer may receive an email via internet connection 216 containing a secure web address link or other instructions for providing the financial account information.

[0047] Other. Alternatively, the customer may receive a text communication via SMS interface 214 or any other available communications interfaces (not shown) containing a link to a secure web address or other instructions for entry of the financial account information.

[0048] In an embodiment, the merchant assigns a unique identification number to the customer, and the identification number or an index entry to the identification number is transmitted to the secure server as part of enrollment information that allows linking the data on the secure server to the particular customer enrollment record on the merchant's server.

[0049] To establish the second data entry session and link it to the appropriate open enrollment session, the customer may be invited to enter a shared secret, such as an assigned access key, partial or complete social security number, account number, telephone number, password, or other data to authenticate the customer for the second session. If the second session is synchronous with the first session (for example, the two data entry points are provided simultaneously on the same

web page or a caller is transferred directly to an IVR system at the conclusion of a debt collection or order taking call) the existence of the connection with the customer for the merchant server data entry may provide sufficient authentication for a direct transfer to the second data entry process, without further authenticating steps. If the two processes are non-synchronous, for example, the second data entry occurs at some later time or even a later date, a further authentication may be appropriate. In an embodiment, the connection instructions and authentication shared secret may be provided to the customer by the secure server 202 without the merchant having such information, thus providing a further level of security to avoid employees of the merchant accessing the second session or its data.

[0050] Embodiments described herein provide significant unobvious advantages. For example, the process disclosed eliminates the possibility of security breaches at the merchant location that would expose financial account data, due to a keystroke logger, camera, or other similar data breach. The financial account information is never provided to the merchant's personnel, nor does it go through the merchant server or network. This mechanism may also reduce the amount of data entry required of the end user and reduce keyboarding errors.

[0051] In an embodiment, the token provided to the merchant is a symbolic representation of a financial instrument or account that is only meaningful to the merchant. Knowledge of this token is required for an authorized user to use the financial instrument or account.

[0052] The secure server 202 or "hosted system" preferably meets acknowledged security standards, such as PCI compliance, to safeguard the financial account information secured there. The secure server 202 processes transactions using this secured information upon receipt of instructions and a token or other customer identifier from the merchant system that identifies the account to be charged.

[0053] Transactions processed may include, for example, credit card, ACH, and any other type of transaction processed using stored financial account information. In addition, other information (beyond financial account information) can be stored in connection with the customer identifier or token. For example, other customer and credit account information may be stored by the host system in connection with the customer record associated with the customer identifier or token. Further, the payee may specify what types of cards are accepted as payment mechanisms. A payee

can decide to accept or not accept various types of cards, such as debit cards, prepaid cards, and cards from particular issuing banks.

[0054] In another example embodiment, the merchant or other payee may provide an incentive for the payer to follow through with the process by entering financial account information for storage in the secure server. Information on an incentive for completing the intended payment setup may be transmitted to the secure server along with the instructions for obtaining the financial account information. The secure server then sends a message to the payer through one or more of the available communications channels (either initially, or in a follow-up message if the process is not completed promptly), offering the payer the indicated incentive. For example, the payer may be offered a discount, a gift, a coupon or voucher for additional goods or services, or any other desired incentive to complete the entry of financial account information and enable an expected payment.

[0055] Figs. 4a through 4l together comprise a multi-page flow chart of a further detailed example embodiment of the system and method disclosed herein. The numbered connecting points in these flow charts correspond to the numbered connecting point the continuing process can be found. The functions performed are indicated in the flow chart blocks.

[0056] Further, the flow charts of Figs. 4a through 4l incorporate "swim lane" information indicating where functions may be performed in the example embodiment. Locations shown include the End User system (for example, systems at location 206, 208 or 210), merchant server 204 (sometimes referred to as the "Payment Application" server), a Web Browser also operating at locations 206, 208, or 210, and the secure server 202 (sometimes referred to as the "Financial Account Registration Application" server). Functions are also divided in the example embodiment of Figure 4a-4l among a calling system ("Integrated System"), and a secure server or combination of servers comprising the API engine (sometimes designated in the flow chart as PayAPI), a payment hub associated with the API engine, and a Financial Account Warehouse (secure storage location). An external credit card network is also connected to the system via a communications channel such as the Internet.

[0057] Those skilled in the art will appreciate that the flow charts provided herein are only one example implementation; functions may be reassigned as desired among the functional parts and locations of the system while remaining within the spirit of the invention.

[0058] The detailed flow chart starts at Fig. 4a with main branch 502, indicating that the URL interface provided may be implemented either with a static URL in step 506 (designated as 1B) or a dynamic URL in step 504 (designated as 1A).

[0059] Figs. 4b and 4c together show the continuing example flow chart for the dynamic URL implementation. Starting at step 508, the end user communicates with the Payment Application running on merchant server 204 to request registration of a financial account. The method then continues with a process of logging into the payment gateway (designated as subroutine "2"), which is disclosed in more detail in Fig. 4f. Next, a financial account registration entry form (designated as subroutine "3") is provided, using a process disclosed in more detail in Fig. 4g. In step 510, the application launches a browser window for the end user with a specified Financial Account Registration URL. In step 512, the end user's web browser initiates a Secure Socket Layer connection to the secure server 202. In step 514, the secure server 202 responds to establish the SSL connection.

[0060] Next, in step 516, the Financial Account Registration Application in secure server 202 dynamically generates financial account registration request form data and transmits this data to the end user's web browser. In step 518, the browser displays the form for the end user.

[0061] The end user, in steps 520 and 522, selects the financial account type to be registered, either credit card or bank account.

[0062] If a credit card is selected, the process continues at step 524 where credit card fields are displayed for the end user. Continuing on Figure 4c, in step 530 the end user inputs card data. Then, in step 534, the browser encrypts the entered card data using SSL protocols. The Financial Account Registration Application confirms the end user's login (designated as Subroutine "2", see Fig. 4f) and performs the card registration process shown in Figs. 4i and 4j (designed as Subroutine "5").

[0063] If a bank account is selected, the process continues from step 522 to step 526 where bank account data entry fields are displayed for the end user. Continuing on Figure 4c, in step 528 the end user inputs bank account data. Then, in step 534, the browser encrypts the entered bank account data using SSL protocols. The Financial Account Registration Application confirms the end user's login (designated as Subroutine "2", see Fig. 4f) and performs the bank account registration process shown in Fig. 4k (designed as Subroutine "6").

[0064] As shown in Figure 4c, regardless of whether a card or bank account was selected for registration, after Subroutine 6 or 7 is processed to register the financial account information, operation continues at step 535 where the financial account registration application parses and logs the response from the appropriate registration subroutine. Next, in step 536, the application sends confirmation codes and a success message to the end user's browser. In an embodiment, the confirmation codes are an array of values presented to the end user during enrollment confirmation that serve as a shared secret between the system and the end user. The confirmation codes may be used in conjunction with the external request ID as a key to retrieving a token from the system.

[0065] The browser displays a confirmation in step 538, and in step 540 the end user's system requests a reference ID that identifies the just-registered card or account. After validating the user's login to the Payment Application (merchant server 204), the reference ID (also referred to as a financial account token) is transmitted to the merchant server 204 using the process in Fig. 4l, (designated as Subroutine "7"). The payment application in the merchant server 204 displays a success message in step 542 and stores the reference ID for future use, in step 544.

[0066] Figs. 4d and 4e combine to show an example flow chart for a static URL implementation. Referring first to Fig. 4d, this process starts at step 546 when the end user requests registration of a financial account. Subroutine "2" is then activated in the merchant server payment application to ensure that the end user is properly identified by the system and that information entered by the end user is associated with the correct user and account. The payment application then displays an array of codes in step 548 and launches a web browser with a financial account registration URL 550.

[0067] In step 552, the end user's browser requests an SSL connection from the indicated static URL pointing to the secure server 202, and in step 554 the financial account registration application establishes the SSL connection. In step 556 the registration application sends account registration request form data in a static form to the browser. Then, the browser displays the static form in step 558. In steps 560 and 562, the end user's system transmits the array of codes (provided by the payment application in step 548) in an encrypted form to the financial account registration application. The financial account registration application then sequentially executes Subroutines "4", "2", and "3". Subroutine "4" implements IP address access and restrictions as shown in Figure

4h. Subroutine "2" verifies identity of the user (see Fig. 4f), and Subroutine "3" obtains the financial account registration entry form (see Fig. 4g).

[0068] Next, in step 564, the financial account registration entry form is transmitted to the end user's browser and rendered in step 566. The end user selects a financial account type in step 568. If a card is selected, the process continues with step 570 and the card registration fields are rendered.

[0069] If a credit card is selected, the process continues in Figure 4e at step 530 where the end user inputs card data. Then, in step 534, the browser encrypts the entered card data using SSL protocols. The Financial Account Registration Application confirms the end user's login (designated in the flow chart as Subroutine "2", see Fig. 4f) and performs the card registration process shown in Figs. 4i and 4j (designated in the flow chart as Subroutine "5").

[0070] If a bank account is selected, the process continues in Figure 4e at step 528 where the end user inputs bank account data. Then, in step 534, the browser encrypts the entered bank account data using SSL protocols. The Financial Account Registration Application confirms the end user's login (designated in the flow chart as Subroutine "2", see Fig. 4f) and performs the bank account registration process shown in Fig. 4k (designated in the flow chart as Subroutine "6").

[0071] Regardless of whether a card or bank account was selected for registration, after subroutine 6 or 7 is processed to register the financial account information, operation continues as shown in Figure 4e at step 535, where the financial account registration application parses and logs the response from the appropriate registration subroutine. Next, in step 536, the application sends confirmation codes and a success message to the end user's browser. The browser displays a confirmation in step 538. In step 539, the array of confirmation codes is provided. In an embodiment, the confirmation codes are an array of values presented to the end user during enrollment confirmation that serve as a shared secret between the system and the end user. The confirmation codes may be used in conjunction with the external request ID as a key to retrieving a token from the system. In step 540 the end user's system uses the confirmation codes to request a reference ID that identifies the just-registered card or account. After validating the user's login to the Payment Application (merchant server 204), the reference ID (also referred to as a financial account token) is transmitted to merchant server 204 using the process in Fig. 4l, (designated as

Subroutine "7"). The payment application in the merchant server 204 displays a success message in step 542 and stores the reference ID for future use, in step 544.

[0072] Fig. 4f shows an example embodiment of a payment gateway login function subroutine, referenced in the various flow charts of Figure 4 as Subroutine "2". Starting at step 573, the routine determines whether the session identifier provided by the end user is valid for a current active session. If so, the process concludes at step 598 and the user is permitted to access the relevant system. If not, a login request method is invoked at step 574. The API then parses the request at step 576, and authenticates the system user at step 578. During step 578 the system may access the organization application and user key registry at step 580. In step 582, the system determines whether the request is authentic.

[0073] If not authentic, an error response is generated in step 592, an error message is displayed in step 594, and the subroutine concludes at step 596 where the user is not permitted to advance, i.e. access the system. If the request is deemed authentic in step 582, the request is validated in step 584 through a validation engine operational step 586. The request is logged and an external request ID is stored in step 588. The external request ID is an input parameter for session requests. In an embodiment, the external request ID serves as a shared secret between the requesting application and the system, and is later used as a key to retrieving a token from the system.

[0074] In step 590, if the validation step 584 indicated a valid request, a login success response occurs at step 604, the session ID is stored at step 606, a success message is transmitted, parsed and displayed in step 600, session ID is stored at step 602, and the user is allowed to advance (step 598). If the request is deemed invalid at step 590, processing continues with steps 592-596 as described previously.

[0075] Figure 4g shows an example process for obtaining a financial account registration entry form. Starting at step 402, the process invokes a method for obtaining the form as established in the API. In step 404 the system stores the external request ID received from the system requesting the collection of financial account information. The API engine in the secure server 202 parses the request in step 406. In step 408, the API validates the request by connecting to the validation engine (step 410). In step 412, the API determines whether the request is valid. If not, an error response is generated in step 414 and an error message is displayed in step 416. If the request is

valid, the process continues at step 418 where the request is checked against any programmed restrictions at the payee level by interacting with the payment hub (step 420) to ensure validity of the request. For example, if the payee has indicated it does not wish to accept credit cards, a request to store credit card information would be invalid. In step 422, the request is similarly checked against any customer-level restrictions on account type, by obtaining data stored in the payment hub (step 424). For example, if a particular category of customer is permitted to pay only with a credit card and not using a bank account, requests outside the permitted operations would be invalid. Then, in step 426, the request is checked against any "customer account level" restrictions on account type, by obtaining data stored in the payment hub (step 428).

[0076] In step 430, the API creates a registration URL and (optionally) establishes an expiration time for the URL. The expiration time may be 5 minutes, 30 minutes, several hours, or a day or more, depending on the nature of the interaction with the payer, which will determine the scope of a "reasonable time" to complete the transaction. In a seamless online transaction, the time allowed might be relatively short, for example, measured in minutes. In a bill collector transaction where the payer has agreed to go online at a later time and enter payment information, the time allowed would be longer, for example, measured in days. In step 432, the URL creation time is logged and the external request ID is stored. In step 434, a success response is generated. In step 436, the calling system receives the success response from the API and logs the response. Then, in step 438, the subroutine is concluded and control advances to the next function in the calling program.

[0077] Figure 4h is a flow chart for Subroutine "4", which verifies IP address access and restrictions. First, in step 440, the IP address seeking access to the system is checked for restrictions, through interaction with a database of restricted addresses (step 442). In step 444, the subroutine branches based on the restrictions found. If the IP address is restricted, then in step 446 an error response is generated and in step 448 the end user's web browser displays the error message. If no restriction is found, the process continues at step 450, and the request is judged as either authentic or not authentic. If the request is authentic, the subroutine terminates at step 452. If the request is not authentic, it is logged at step 454 and the time of the request is recorded in step 456. In step 458, the history of requests from the IP address is reviewed with reference to a request log (step 460). In step 462, if the number of allowed failed requests in a given time period has not been exceeded, the subroutine terminates at step 452. If the number of allowed failed requests

from an IP address has been exceeded, the IP address is added to the restricted list in step 464, a lockout is established in step 466, and a lockout message is displayed in step 468.

[0078] Figs. 4i and 4j (taken together) comprise a flow chart showing the card account registration process, referenced as Subroutine "5". Referring first to Fig. 4i, the system initially invokes an API method to add a credit card account, in step 470. In step 472, the external request ID associated with the customer is stored. In step 474, the API engine parses the request and in step 476, validates the request. If the request is invalid in step 478, an error response is generated in step 480, and the error message is displayed in step 482. The subroutine then terminates in step 484 without registering a card.

[0079] If the request is valid in step 478, an authorization request is generated in step 486, and the request is logged in step 487.

[0080] Continuing in Figure 4j, the authorization request is processed by the card network in step 488 and a response is generated in step 489. The API engine receives the response and parses it and records it, in step 490. If the card data was authorized, in step 491, an approval response is generated in step 495, the approval response is transmitted to the calling system in step 496, and the subroutine terminates in step 497. Also, in case of authorization, the payment hub logs the response and stores the reference ID. The financial account secure server (referred to as the "warehouse") stores the financial account information (card information) and the external request ID in step 499.

[0081] If the credit card is not authorized in step 491, a decline response is generated in step 492, an error message is displayed for the user in step 493, and the subroutine terminates at step 494 without storing card information.

[0082] Figure 4k is a flow chart for the bank account registration subroutine (referenced as subroutine "6"). In step 608, the add bank account method of the API is invoked by the calling system, and the external request ID is stored in step 612. In step 610, the API engine parses the request and validates it in step 614 by communicating with a validation engine (step 616). Step 618 determines whether the request is valid. If so, an approval response is generated in step 630. Then, in step 632 the request is logged, the external request ID is stored, and the reference ID is stored, and in step 634 the bank account information and external request ID are stored in the

secure server. At the same time, in step 628, the approval response is received by the calling system and parsed and logged, whereupon the subroutine terminates at step 626.

[0083] If the request is not valid in step 618, an error response is generated at step 620, the response is transmitted to the calling system, where it is parsed at step 622 and displayed, and the subroutine terminates at step 624 without storing any bank account information.

[0084] Figure 4l is a subroutine for a process of obtaining a financial account token. In step 636, the get token request method of the API is invoked by the calling system. The API engine parses the request in step 646 and validates it in step 648. If the request format is invalid, an error response is generated in step 652 and an error message is displayed in step 640, whereupon the subroutine terminates. If the request format is valid, the financial account reference ID(s) are retrieved in step 654, and a success response is generated in step 656. The response is parsed by the calling system in step 642 and the subroutine terminates in step 644.

[0085] The programmed functions implementing the methods and processes described herein can be provided in a variety of forms. In one preferred embodiment, as noted previously, the functions provided by secure server 202 may be accessed in the form of an API defining functions available to the merchant server 204. These functions may be implemented in the manner described in United States Provisional Patent Application Serial No. 61/655,482 filed June 5, 2012 and United States Provisional Patent Application Serial No. 61/698,574 filed September 8, 2012, the disclosures of which are incorporated herein by reference. Those skilled in the art will appreciate that the method of defining the API and the particular API features provided may be varied as desired within the scope of the invention, to implement desired concepts described herein and variations on those concepts that will be apparent to those skilled in the art after reviewing this specification.

[0086] The screen displays described herein may be designed in any desired manner consistent with achieving the goals of a particular variation, and the screen displays may take various forms without departing from the scope or spirit of the invention. For example, the screen displays may have the form disclosed in United States Provisional Patent Application Serial No. 61/655,482 filed June 5, 2012 and United States Provisional Patent Application Serial No. 61/698,574 filed September 8, 2012, the disclosures of which are incorporated herein by reference.

[0087] Although illustrative embodiments have been described herein in detail, it should be noted and understood that the descriptions and drawings have been provided for purposes of illustration only and that other variations both in form and detail can be added thereto without departing from the spirit and scope of the invention. The terms and expressions in this disclosure have been used as terms of description and not terms of limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the claims and their equivalents. The terms and expressions herein should not be interpreted to exclude any equivalents of features shown and described, or portions thereof.

We claim:

1. A method of processing a payment from a payer to a payee operating a first computing system, the method being performed by a second computing system, the method comprising:

receiving an electronically-generated payment transaction instruction from the first computing system, wherein the payment transaction instruction:

includes at least one data element associated with the payer;

specifies the amount of the payment from the payer to the payee; and

specifies a communications link for the second computing system to obtain financial account information from the payer;

obtaining the financial account information from the payer via the specified communications link;

generating an electronic data token representing the financial account information obtained from the payer;

outputting the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer;

storing the financial account information obtained from the payer;

obtaining the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer; and

forwarding at least a portion of the amount of the payment to the payee.

2. The method of claim 1, further comprising:

receiving a second payment transaction instruction from the first computing system, wherein the second payment transaction instruction:

includes a representation of the electronic data token; and

specifies the amount of the second payment from the payer to the payee;

processing the second payment using the financial account information represented by the electronic data token; and

forwarding the amount of the second payment to the payee.

3. The method of claim 1, wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used by the first computing system to obtain enrollment data from the payer.

4. The method of claim 1, wherein the communications link is at least one of a telephone number to enable the second computing system to communicate with the payer and obtain the financial account information or a transfer from an existing telephone call with the payer to a telephone system that receives the financial account information from the payer.

5. The method of claim 1, wherein the communication link is a connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system.

6. The method of claim 5, wherein the connection is a widget or window within a website provided by the first computing system.

7. The method of claim 5, wherein the connection provides access to the second computing system using a static or dynamic universal resource locator (URL).

8. The method of claim 1, wherein the communications link used to obtain the financial account information from the payer is asynchronous with a communications link used by the first computing system to obtain enrollment data from the payer.

9. The method of claim 8, wherein the payment transaction instruction for the second computing system to obtain the financial account information from the payer includes data sufficient for the second computing system to authenticate the payer.

10. The method of claim 9, wherein the first computing system defines a period of persistence for the second computing system to obtain the financial account information from the payer.

11. The method of claim 1, wherein the payment transaction instruction comprises contact information for the payer to enable the second computing system to transmit instructions to the payer for communicating the financial account information to the second computing system.

12. The method of claim 11, wherein the contact information comprises one of an email address or a telephone number whereby the second computing system sends a link for a data entry connection to the payer via one of email and text.

13. The method of claim 1, wherein the financial account information includes at least one of a credit card number or bank account number.

14. A second computing system that processes a payment from a payer to a payee operating a first computing system, the second computing system comprising:

one or more processors; and

memory storing instructions that, when executed by the one or more processors, cause the second computing system to:

receive an electronically-generated payment transaction instruction from a first computing system, wherein the payment transaction instruction:

includes at least one data element associated with the payer;

specifies the amount of the payment from the payer to the payee; and

specifies a communications link for the second computing system to obtain financial account information from the payer;

obtain the financial account information from the payer via the specified communications link;

generate an electronic data token representing the financial account information obtained from the payer;

output the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer;

store the financial account information obtained from the payer;

obtain the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer; and

forward at least a portion of the amount of the payment to the payee.

15. The system of claim 14, wherein the instructions further cause the second computing system to:

receive a second payment transaction instruction from the first computing system, wherein the second payment transaction instruction:

includes a representation of the electronic data token; and

specifies the amount of the second payment from the payer to the payee;

obtain the amount of the second payment from the payer by processing the second payment using the financial account information represented by the electronic data token; and

forward at least a portion of the amount of the second payment to the payee.

16. The system of claim 14, wherein the communications link used to obtain the financial account information from the payer is synchronous with a communications link used by the first computing system to obtain enrollment data from the payer.

17. The system of claim 14, wherein the communication link is a connection via the internet between the second computing system and a computing system used by the payer enabling the payer to input the financial account information for transmittal to the second computing system.

18. The system of claim 17, wherein the connection is a widget or window within a website provided by the first computing system.

19. The system of claim 17, wherein the connection provides access to the second computing system using a static or dynamic universal resource locator (URL).

20. The system of claim 14, wherein the communications link used to obtain the financial account information from the payer is asynchronous with a communications link used by the first computing system to obtain enrollment data from the payer.

21. The system of claim 20, wherein the payment transaction instruction for the second computing system to obtain the financial account information from the payer includes data sufficient for the second computing system to authenticate the payer.

22. The system of claim 21, wherein the first computing system defines a period of persistence for the second computing system to obtain the financial account information from the payer.

23. The system of claim 14, wherein the payment transaction instruction comprises contact information for the payer to enable the second computing system to transmit instructions to the payer for communicating the financial account information to the second computing system.

24. The system of claim 14, wherein the financial account information includes at least one of a credit card number or bank account number.

25. A non-transitory computer readable storage medium storing instructions that, when executed by a processor, cause a second computing system that processes a payment from a payer to a payee operating a first computing system to:

receive an electronically-generated payment transaction instruction from the first computing system, wherein the payment transaction instruction:

includes at least one data element associated with the payer;

specifies the amount of the payment from the payer to the payee; and

specifies a communications link for the second computing system to obtain financial account information from the payer;

obtain the financial account information from the payer via the specified communications link;

generate an electronic data token representing the financial account information obtained from the payer;

output the electronic data token to a communications network for transmittal to the first computing system, wherein the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer;

store the financial account information obtained from the payer;

obtain the amount of the payment from the payer by processing the payment using the financial account information obtained from the payer; and

forward at least a portion of the amount of the payment to the payee.

ABSTRACT OF THE DISCLOSURE

Processing a payment from a payer to a payee (operating a first computing system), by a second computing system, by receiving an electronically-generated payment transaction instruction (identifying the payer, specifying the amount of the payment, and specifying a communications link for the second computing system to obtain financial account information from the payer) from the first computing system, obtaining the financial account information from the payer via the specified communications link, generating an electronic data token representing the financial account information, outputting the electronic data token for transmittal to the first computing system (where the first computing system does not receive the financial account information and the second computing system does not provide the electronic data token to the payer), obtaining the amount from the payer using the financial account information, and forwarding at least a portion of the amount to the payee.

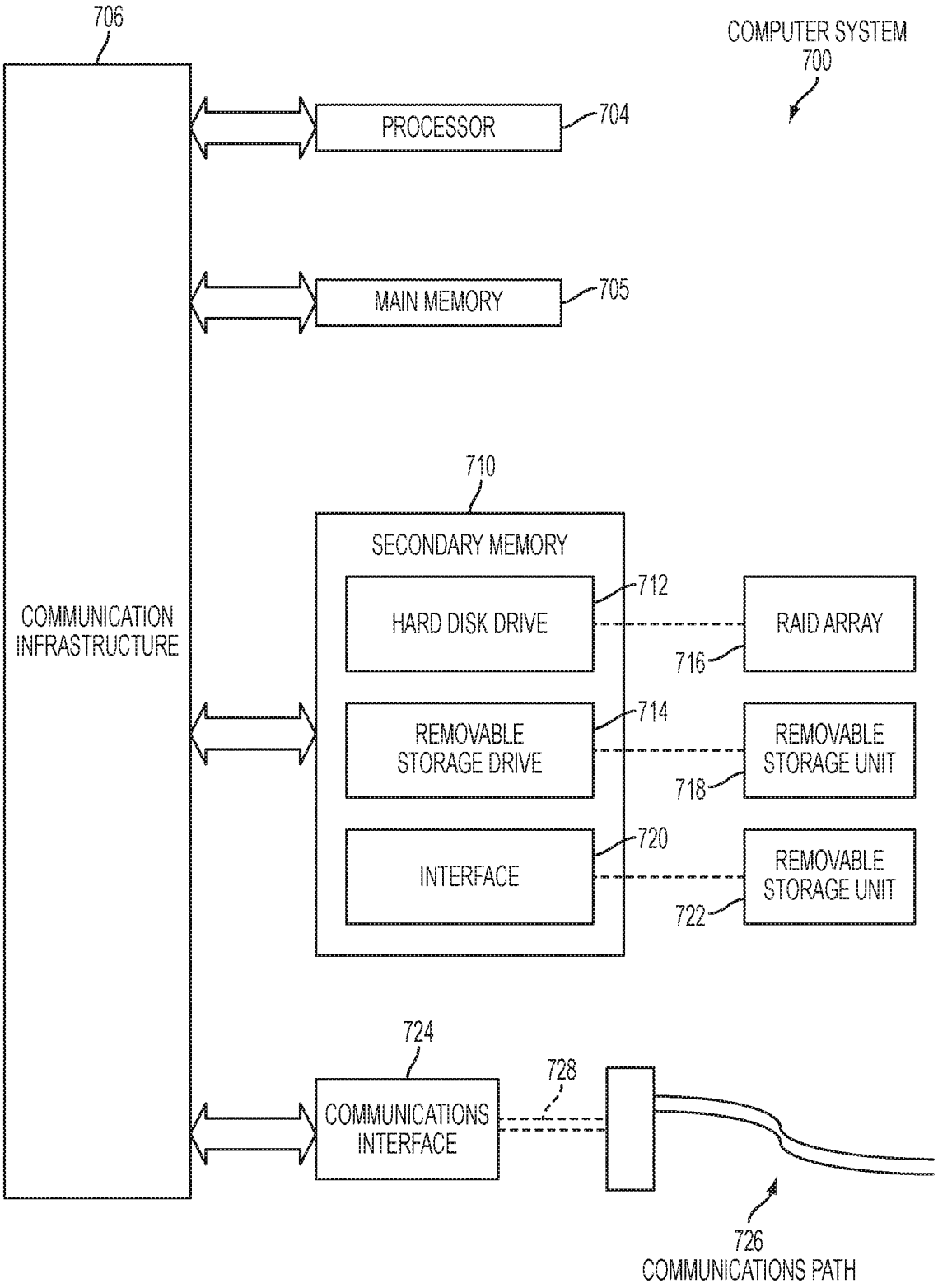

706
COMPUTER SYSTEM
700
PROCESSOR
704
MAIN MEMORY
705
710
SECONDARY MEMORY
HARD DISK DRIVE
712
RAID ARRAY
716
REMOVABLE STORAGE DRIVE
714
REMOVABLE STORAGE UNIT
718
INTERFACE
720
REMOVABLE STORAGE UNIT
722
COMMUNICATION INFRASTRUCTURE
724
COMMUNICATIONS INTERFACE
728
726
COMMUNICATIONS PATH

FIG. 1

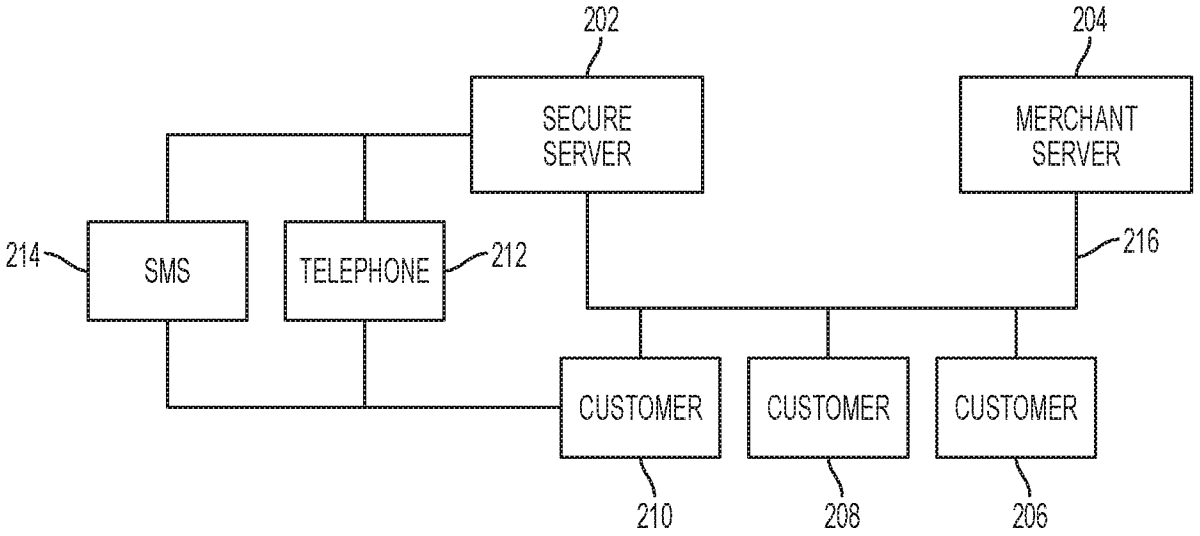

202
204
SECURE SERVER
MERCHANT SERVER
214
SMS
TELEPHONE
212
216
CUSTOMER
CUSTOMER
CUSTOMER
210
208
206

FIG. 2

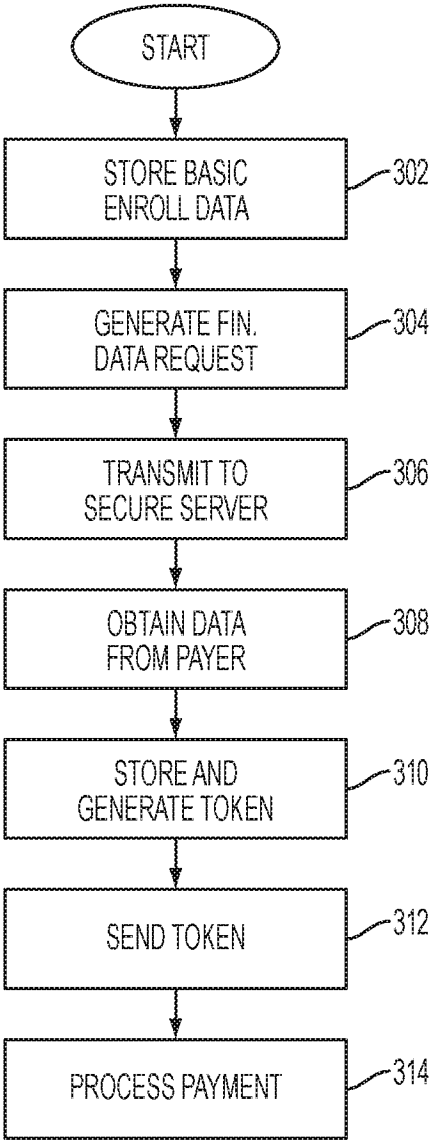

START
STORE BASIC ENROLL DATA
302
GENERATE FIN. DATA REQUEST
304
TRANSMIT TO SECURE SERVER
306
OBTAIN DATA FROM PAYER
308
STORE AND GENERATE TOKEN
310
SEND TOKEN
312
PROCESS PAYMENT
314

FIG. 3

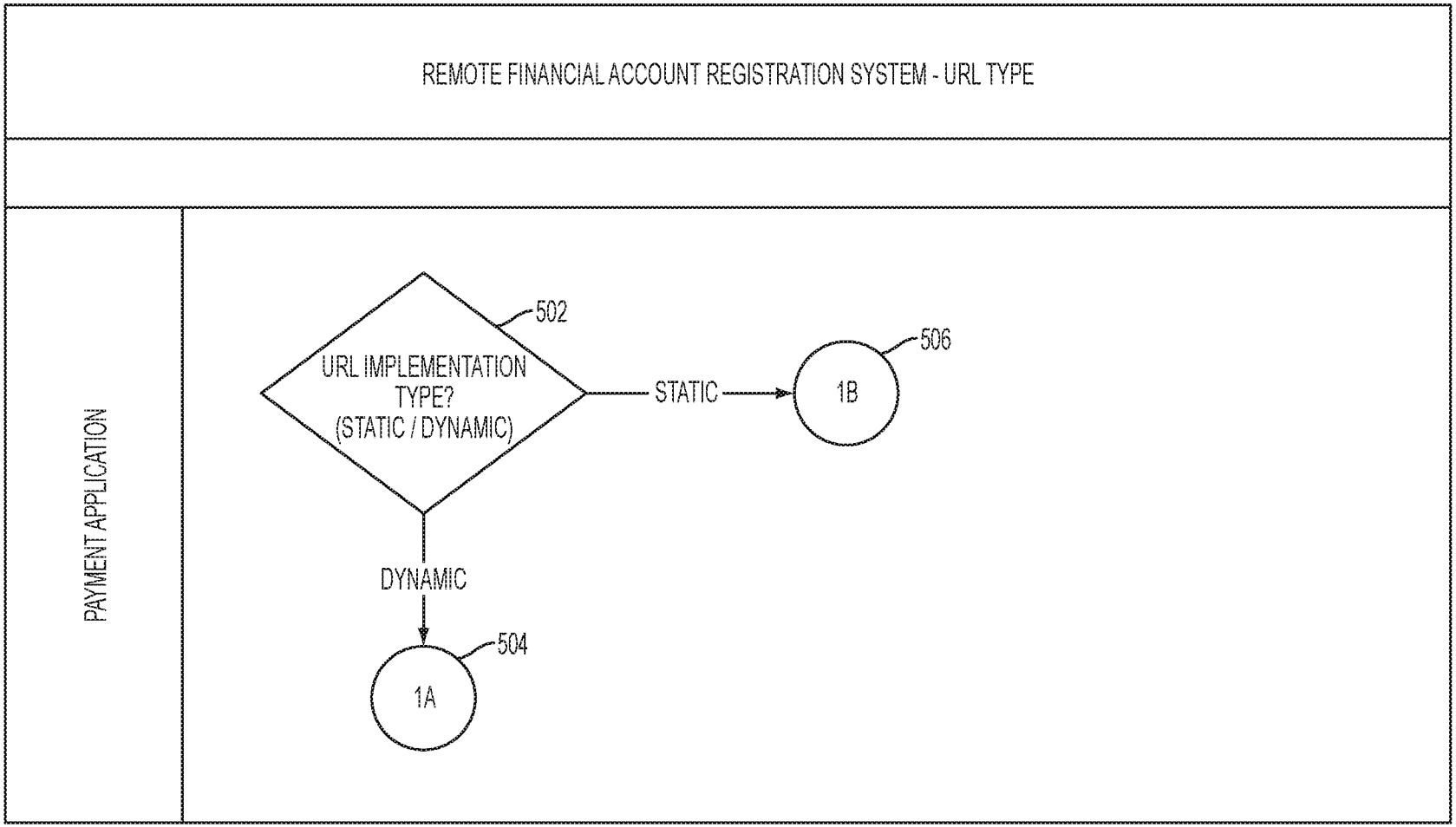

REMOTE FINANCIAL ACCOUNT REGISTRATION SYSTEM - URL TYPE
PAYMENT APPLICATION
502
URL IMPLEMENTATION TYPE? (STATIC / DYNAMIC)
STATIC
506
1B
DYNAMIC
504
1A

FIG. 4a

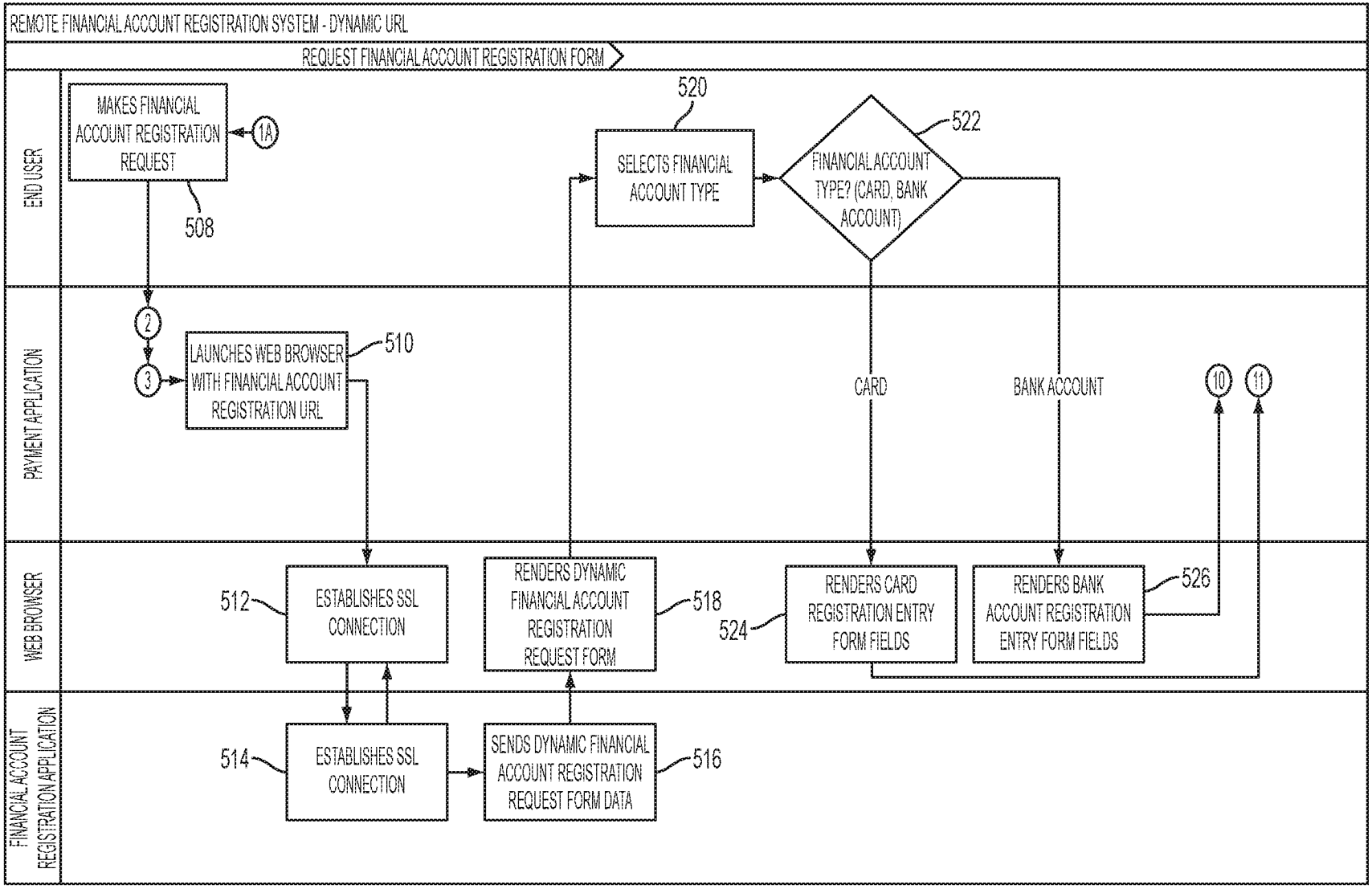

REMOTE FINANCIAL ACCOUNT REGISTRATION SYSTEM - DYNAMIC URL
REQUEST FINANCIAL ACCOUNT REGISTRATION FORM
END USER
PAYMENT APPLICATION
WEB BROWSER
FINANCIAL ACCOUNT REGISTRATION APPLICATION
MAKES FINANCIAL ACCOUNT REGISTRATION REQUEST
1A
508
520
SELECTS FINANCIAL ACCOUNT TYPE
522
FINANCIAL ACCOUNT TYPE? (CARD, BANK ACCOUNT)
2
3
LAUNCHES WEB BROWSER WITH FINANCIAL ACCOUNT REGISTRATION URL
510
CARD
BANK ACCOUNT
10
11
512
ESTABLISHES SSL CONNECTION
RENDERS DYNAMIC FINANCIAL ACCOUNT REGISTRATION REQUEST FORM
518
524
RENDERS CARD REGISTRATION ENTRY FORM FIELDS
RENDERS BANK ACCOUNT REGISTRATION ENTRY FORM FIELDS
526
514
ESTABLISHES SSL CONNECTION
SENDS DYNAMIC FINANCIAL ACCOUNT REGISTRATION REQUEST FORM DATA
516

FIG. 4b

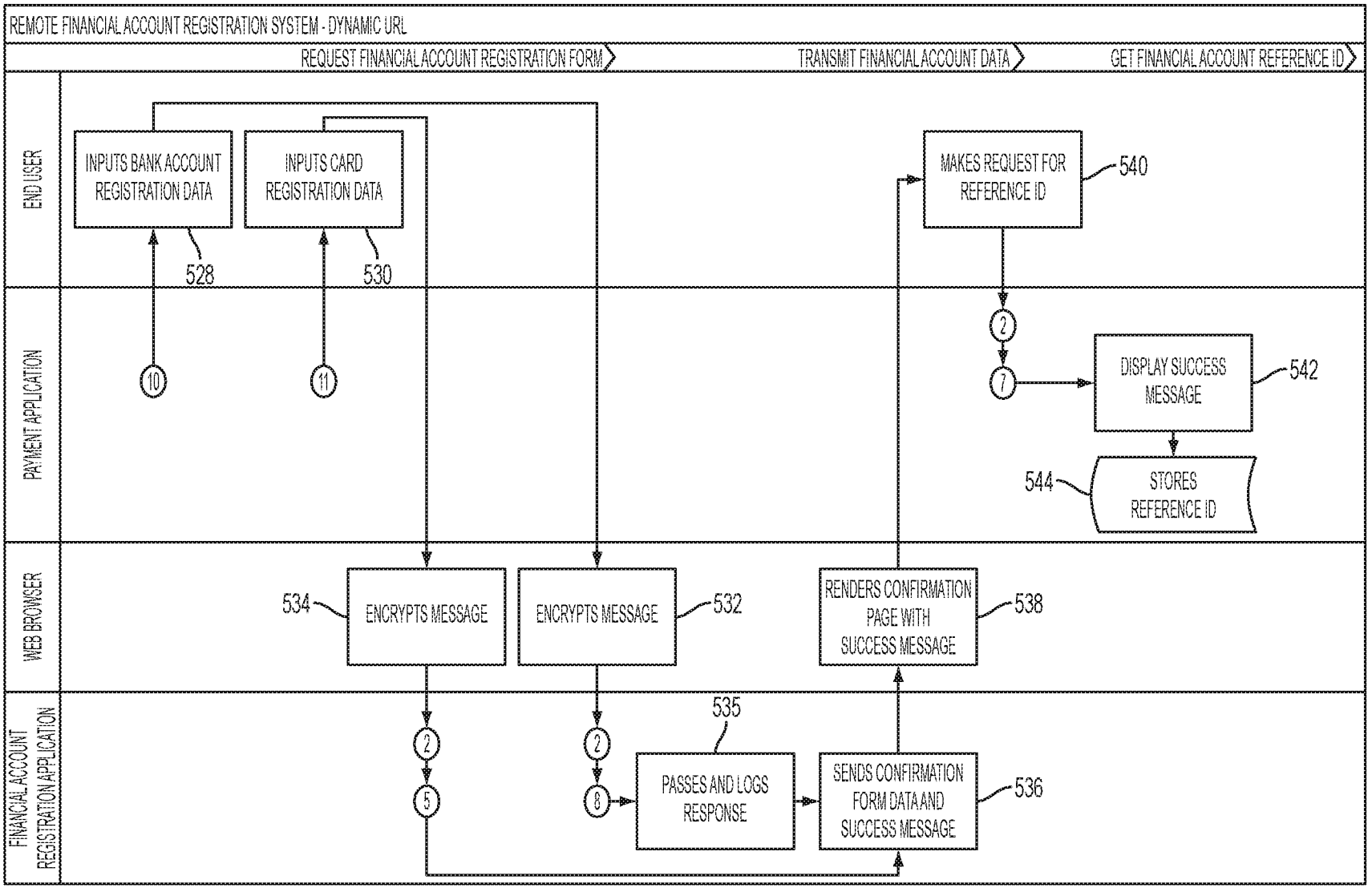

REMOTE FINANCIAL ACCOUNT REGISTRATION SYSTEM - DYNAMIC URL
REQUEST FINANCIAL ACCOUNT REGISTRATION FORM
TRANSMIT FINANCIAL ACCOUNT DATA
GET FINANCIAL ACCOUNT REFERENCE ID
END USER
PAYMENT APPLICATION
WEB BROWSER
FINANCIAL ACCOUNT REGISTRATION APPLICATION
INPUTS BANK ACCOUNT REGISTRATION DATA
528
INPUTS CARD REGISTRATION DATA
530
MAKES REQUEST FOR REFERENCE ID
540
DISPLAY SUCCESS MESSAGE
542
STORES REFERENCE ID
544
ENCRYPTS MESSAGE
534
ENCRYPTS MESSAGE
532
RENDERS CONFIRMATION PAGE WITH SUCCESS MESSAGE
538
535
PASSES AND LOGS RESPONSE
SENDS CONFIRMATION FORM DATA AND SUCCESS MESSAGE
536
10
11
2
7
2
5
2
8

FIG. 4c

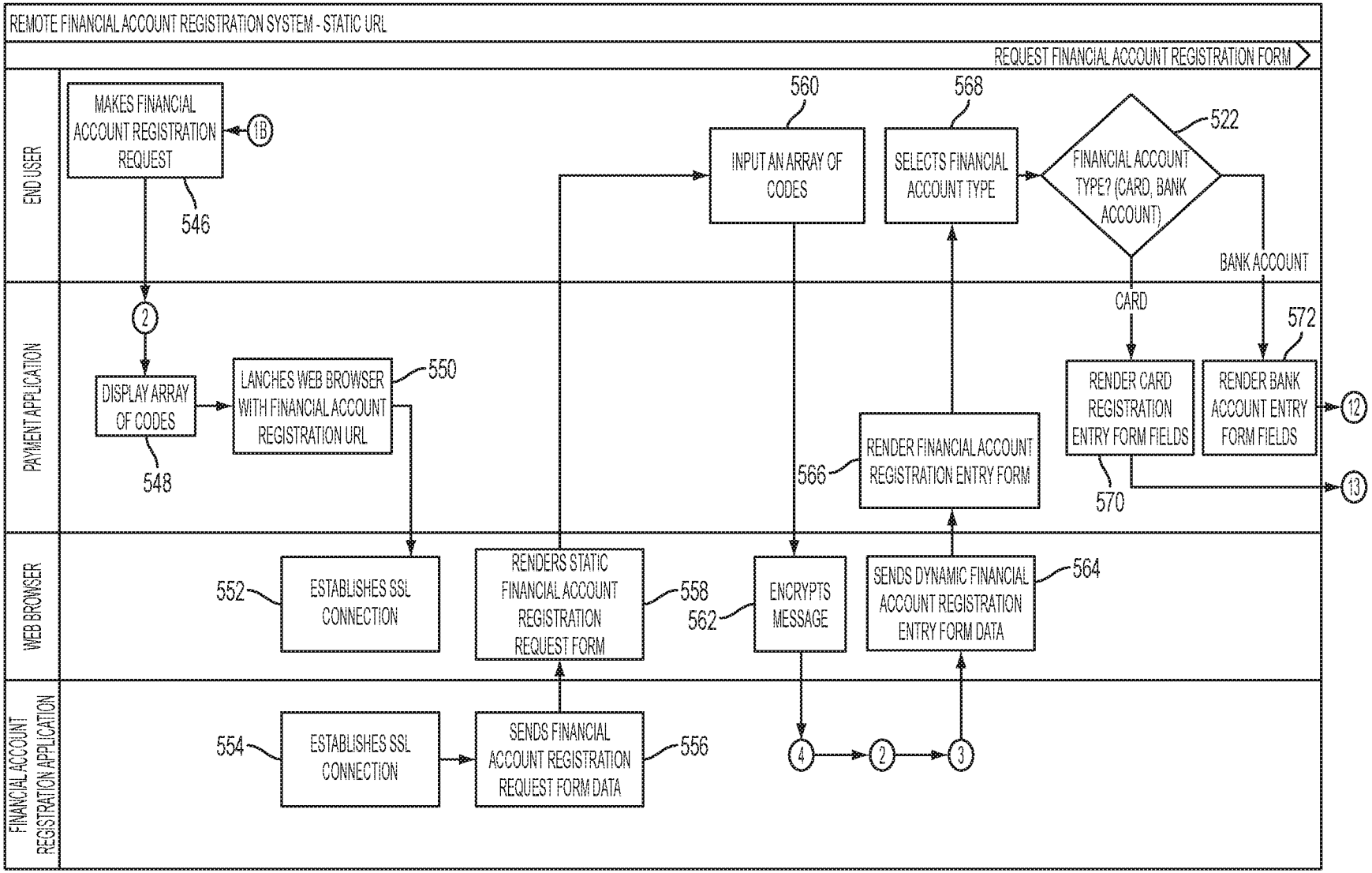

REMOTE FINANCIAL ACCOUNT REGISTRATION SYSTEM - STATIC URL
REQUEST FINANCIAL ACCOUNT REGISTRATION FORM
END USER
PAYMENT APPLICATION
WEB BROWSER
FINANCIAL ACCOUNT REGISTRATION APPLICATION
MAKES FINANCIAL ACCOUNT REGISTRATION REQUEST
1B
546
2
DISPLAY ARRAY OF CODES
548
LANCHES WEB BROWSER WITH FINANCIAL ACCOUNT REGISTRATION URL
550
ESTABLISHES SSL CONNECTION
552
ESTABLISHES SSL CONNECTION
554
SENDS FINANCIAL ACCOUNT REGISTRATION REQUEST FORM DATA
556
RENDERS STATIC FINANCIAL ACCOUNT REGISTRATION REQUEST FORM
558
INPUT AN ARRAY OF CODES
560
ENCRYPTS MESSAGE
562
RENDER FINANCIAL ACCOUNT REGISTRATION ENTRY FORM
566
SELECTS FINANCIAL ACCOUNT TYPE
568
SENDS DYNAMIC FINANCIAL ACCOUNT REGISTRATION ENTRY FORM DATA
564
FINANCIAL ACCOUNT TYPE? (CARD, BANK ACCOUNT)
522
CARD
BANK ACCOUNT
RENDER CARD REGISTRATION ENTRY FORM FIELDS
570
RENDER BANK ACCOUNT ENTRY FORM FIELDS
572
12
13
4
2
3

FIG. 4d

7/15

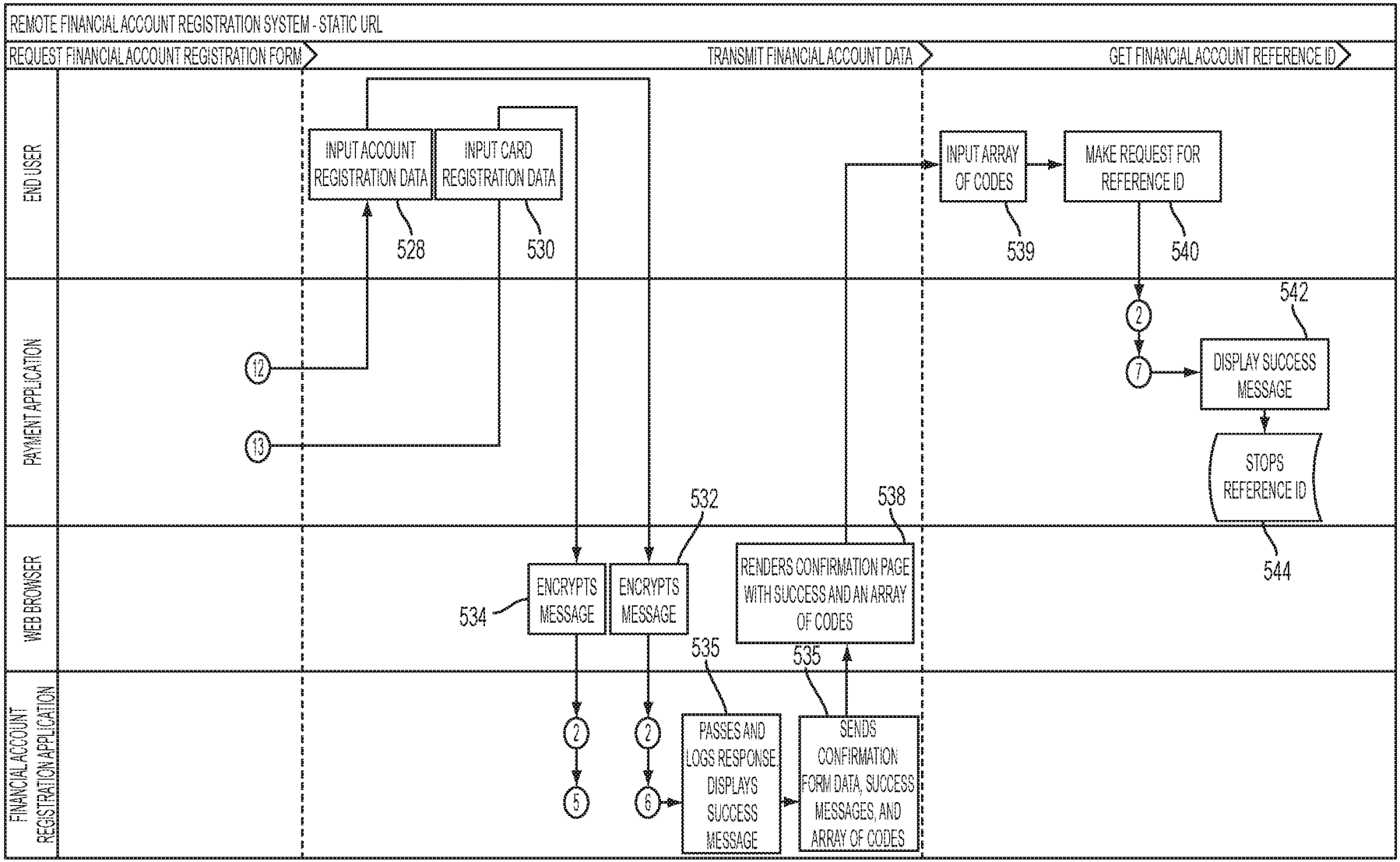

REMOTE FINANCIAL ACCOUNT REGISTRATION SYSTEM - STATIC URL
REQUEST FINANCIAL ACCOUNT REGISTRATION FORM
TRANSMIT FINANCIAL ACCOUNT DATA
GET FINANCIAL ACCOUNT REFERENCE ID
END USER
PAYMENT APPLICATION
WEB BROWSER
FINANCIAL ACCOUNT REGISTRATION APPLICATION
INPUT ACCOUNT REGISTRATION DATA
INPUT CARD REGISTRATION DATA
528
530
INPUT ARRAY OF CODES
MAKE REQUEST FOR REFERENCE ID
539
540
542
DISPLAY SUCCESS MESSAGE
STOPS REFERENCE ID
544
12
13
2
7
532
538
534
ENCRYPTS MESSAGE
ENCRYPTS MESSAGE
RENDERS CONFIRMATION PAGE WITH SUCCESS AND AN ARRAY OF CODES
535
535
2
2
5
6
PASSES AND LOGS RESPONSE DISPLAYS SUCCESS MESSAGE
SENDS CONFIRMATION FORM DATA, SUCCESS MESSAGES, AND ARRAY OF CODES

FIG. 4e

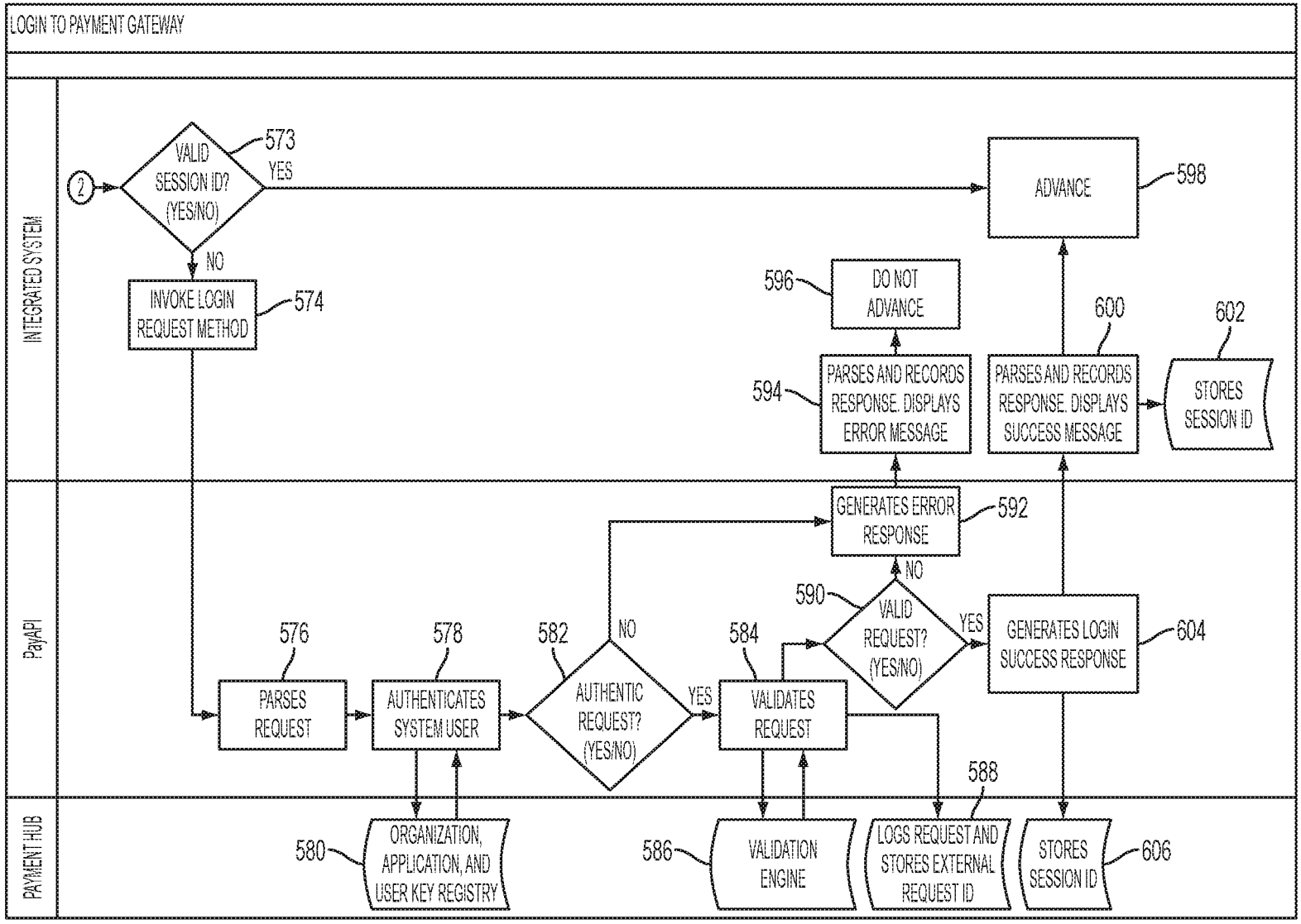

LOGIN TO PAYMENT GATEWAY
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
2
VALID SESSION ID? (YES/NO)
573
YES
NO
INVOKE LOGIN REQUEST METHOD
574
ADVANCE
598
596
DO NOT ADVANCE
600
602
594
PARSES AND RECORDS RESPONSE. DISPLAYS ERROR MESSAGE
PARSES AND RECORDS RESPONSE. DISPLAYS SUCCESS MESSAGE
STORES SESSION ID
GENERATES ERROR RESPONSE
592
NO
590
VALID REQUEST? (YES/NO)
YES
GENERATES LOGIN SUCCESS RESPONSE
604
576
578
582
584
PARSES REQUEST
AUTHENTICATES SYSTEM USER
AUTHENTIC REQUEST? (YES/NO)
NO
YES
VALIDATES REQUEST
588
580
ORGANIZATION, APPLICATION, AND USER KEY REGISTRY
586
VALIDATION ENGINE
LOGS REQUEST AND STORES EXTERNAL REQUEST ID
STORES SESSION ID
606

FIG. 4f

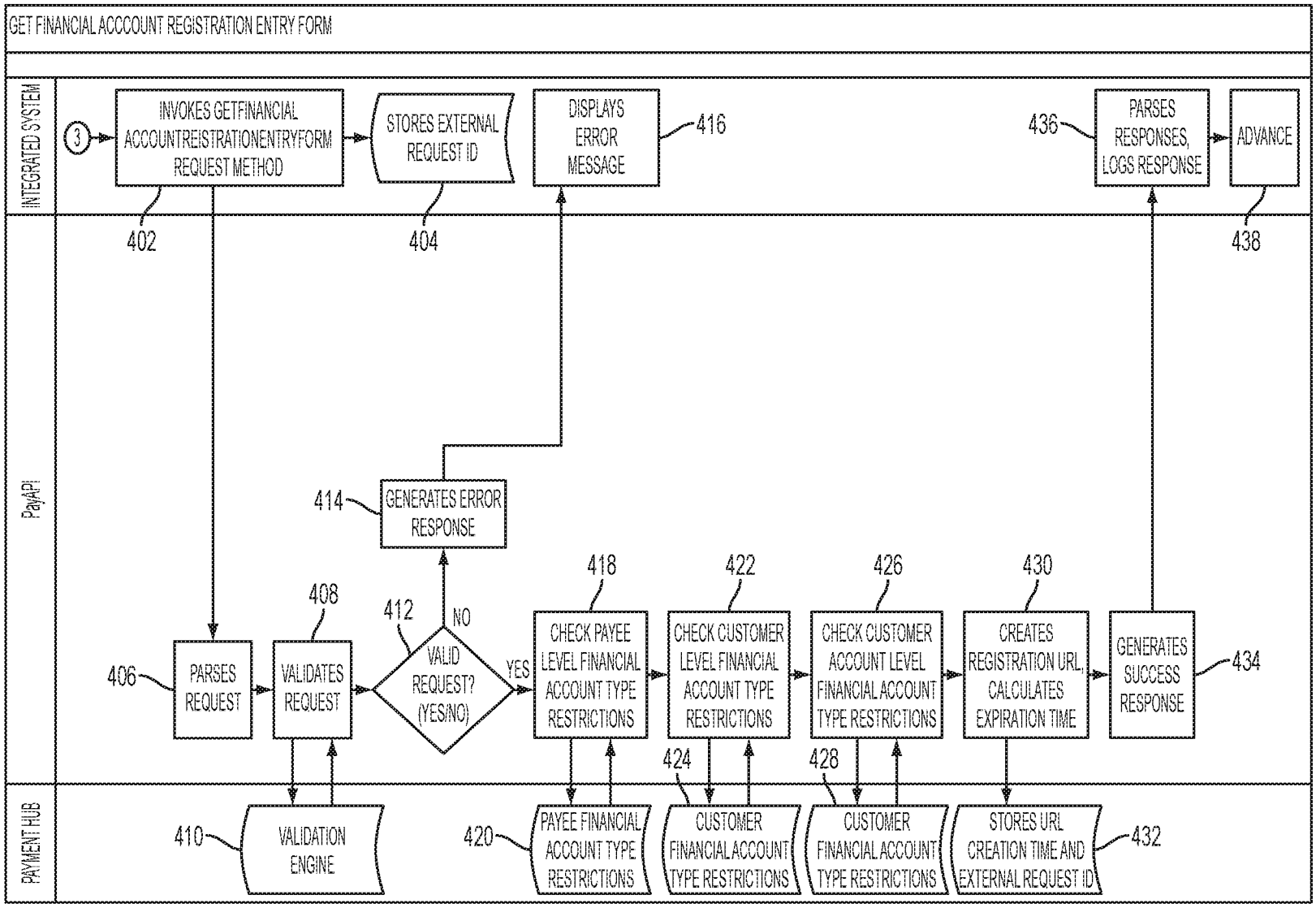

GET FINANCIAL ACCCOUNT REGISTRATION ENTRY FORM
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
3
INVOKES GETFINANCIAL ACCOUNTREISTRATIONENTRYFORM REQUEST METHOD
STORES EXTERNAL REQUEST ID
DISPLAYS ERROR MESSAGE
416
436
PARSES RESPONSES, LOGS RESPONSE
ADVANCE
402
404
438
414
GENERATES ERROR RESPONSE
418
422
426
430
408
412
NO
406
PARSES REQUEST
VALIDATES REQUEST
VALID REQUEST? (YES/NO)
YES
CHECK PAYEE LEVEL FINANCIAL ACCOUNT TYPE RESTRICTIONS
CHECK CUSTOMER LEVEL FINANCIAL ACCOUNT TYPE RESTRICTIONS
CHECK CUSTOMER ACCOUNT LEVEL FINANCIAL ACCOUNT TYPE RESTRICTIONS
CREATES REGISTRATION URL, CALCULATES EXPIRATION TIME
GENERATES SUCCESS RESPONSE
434
424
428
410
VALIDATION ENGINE
420
PAYEE FINANCIAL ACCOUNT TYPE RESTRICTIONS
CUSTOMER FINANCIAL ACCOUNT TYPE RESTRICTIONS
CUSTOMER FINANCIAL ACCOUNT TYPE RESTRICTIONS
STORES URL CREATION TIME AND EXTERNAL REQUEST ID
432

FIG. 4g

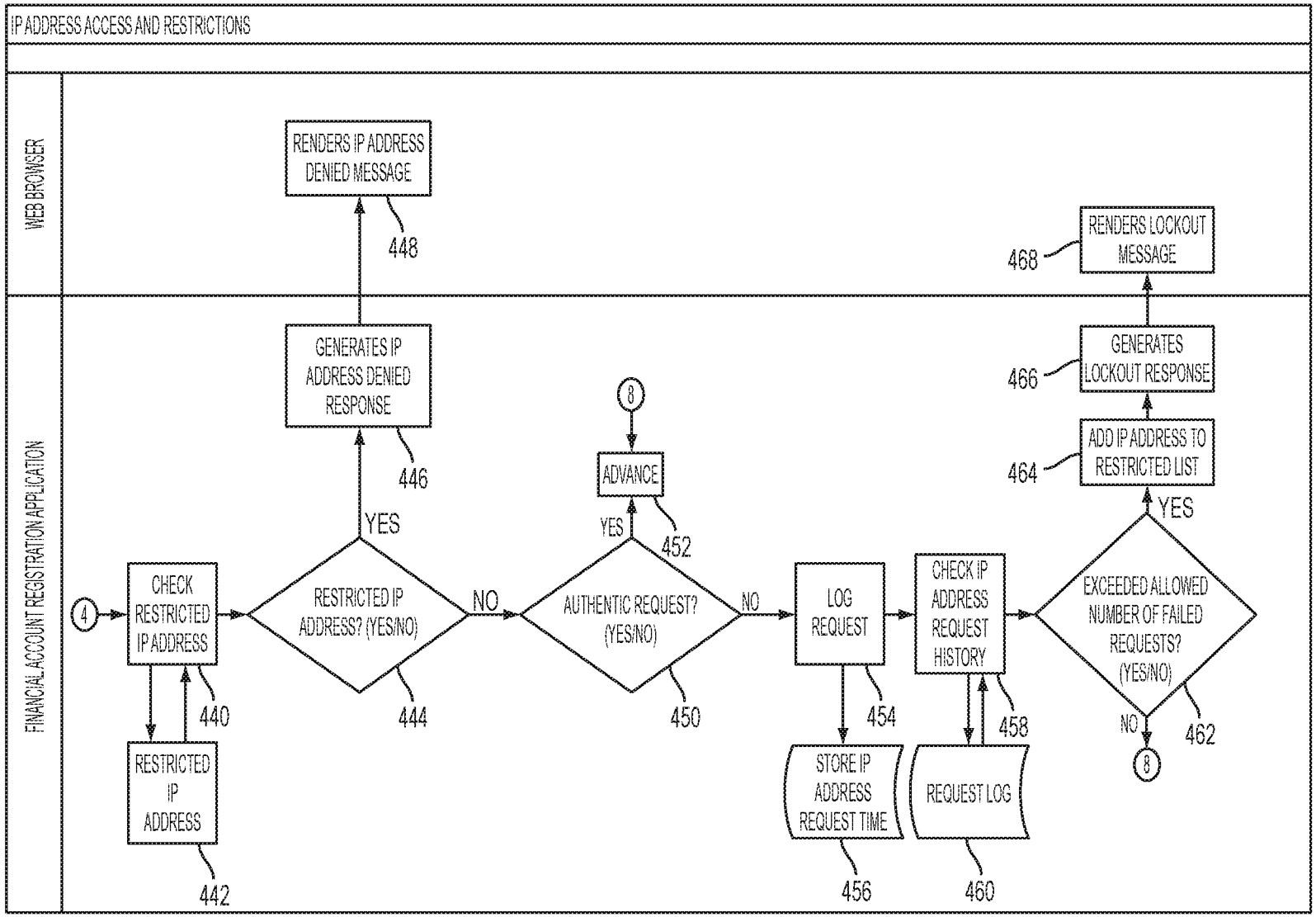

IP ADDRESS ACCESS AND RESTRICTIONS
WEB BROWSER
FINANCIAL ACCOUNT REGISTRATION APPLICATION
RENDERS IP ADDRESS DENIED MESSAGE
448
GENERATES IP ADDRESS DENIED RESPONSE
446
YES
4
CHECK RESTRICTED IP ADDRESS
440
RESTRICTED IP ADDRESS
442
RESTRICTED IP ADDRESS? (YES/NO)
444
NO
8
ADVANCE
YES
452
AUTHENTIC REQUEST? (YES/NO)
450
NO
LOG REQUEST
454
STORE IP ADDRESS REQUEST TIME
456
CHECK IP ADDRESS REQUEST HISTORY
458
REQUEST LOG
460
EXCEEDED ALLOWED NUMBER OF FAILED REQUESTS? (YES/NO)
YES
462
NO
8
ADD IP ADDRESS TO RESTRICTED LIST
464
GENERATES LOCKOUT RESPONSE
466
RENDERS LOCKOUT MESSAGE
468

FIG. 4h

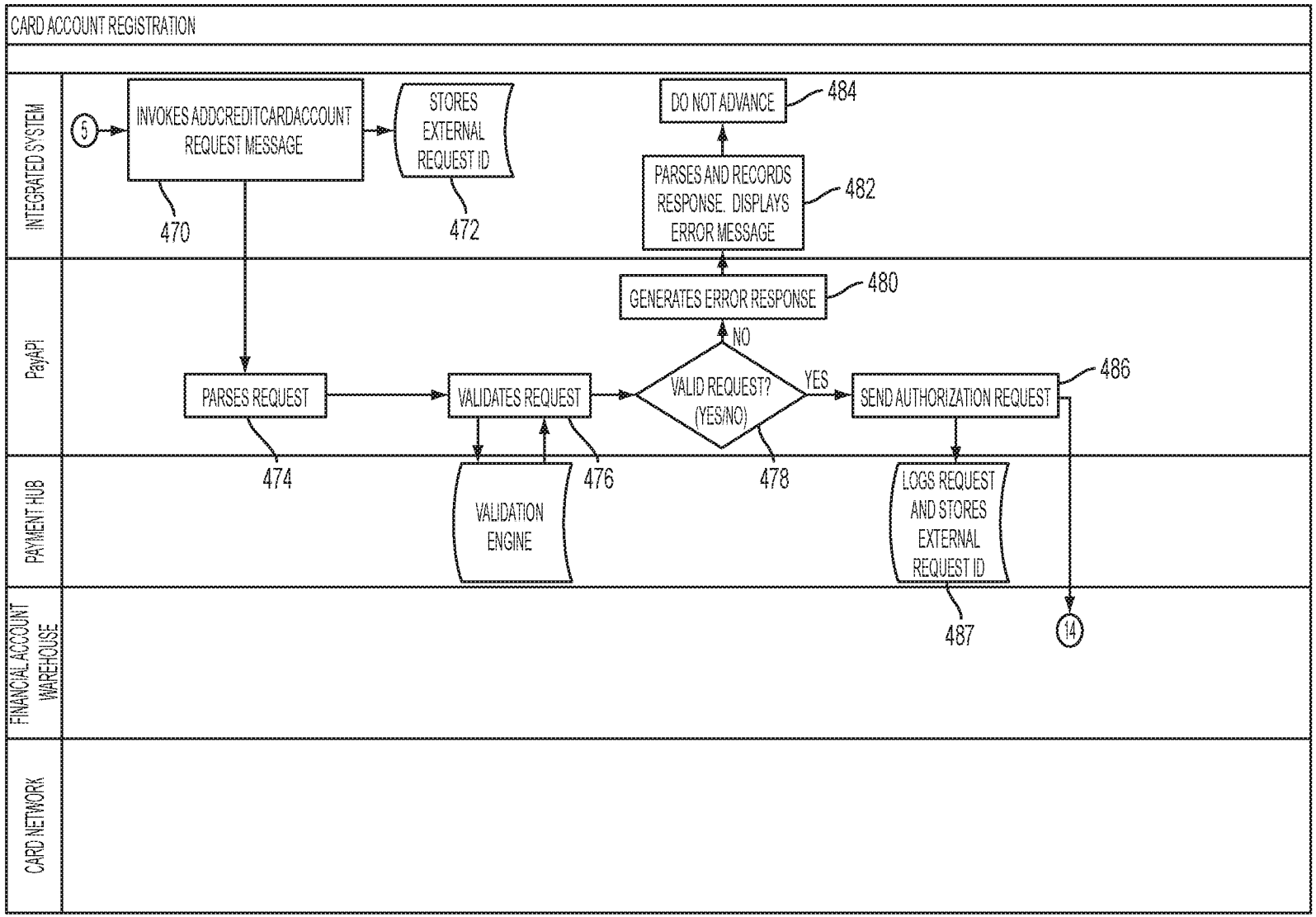

CARD ACCOUNT REGISTRATION
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
FINANCIAL ACCOUNT WAREHOUSE
CARD NETWORK
5
INVOKES ADDCREDITCARDACCOUNT REQUEST MESSAGE
470
STORES EXTERNAL REQUEST ID
472
DO NOT ADVANCE
484
PARSES AND RECORDS RESPONSE. DISPLAYS ERROR MESSAGE
482
GENERATES ERROR RESPONSE
480
NO
PARSES REQUEST
474
VALIDATES REQUEST
476
VALIDATION ENGINE
VALID REQUEST? (YES/NO)
478
YES
SEND AUTHORIZATION REQUEST
486
LOGS REQUEST AND STORES EXTERNAL REQUEST ID
487
14

FIG. 4i

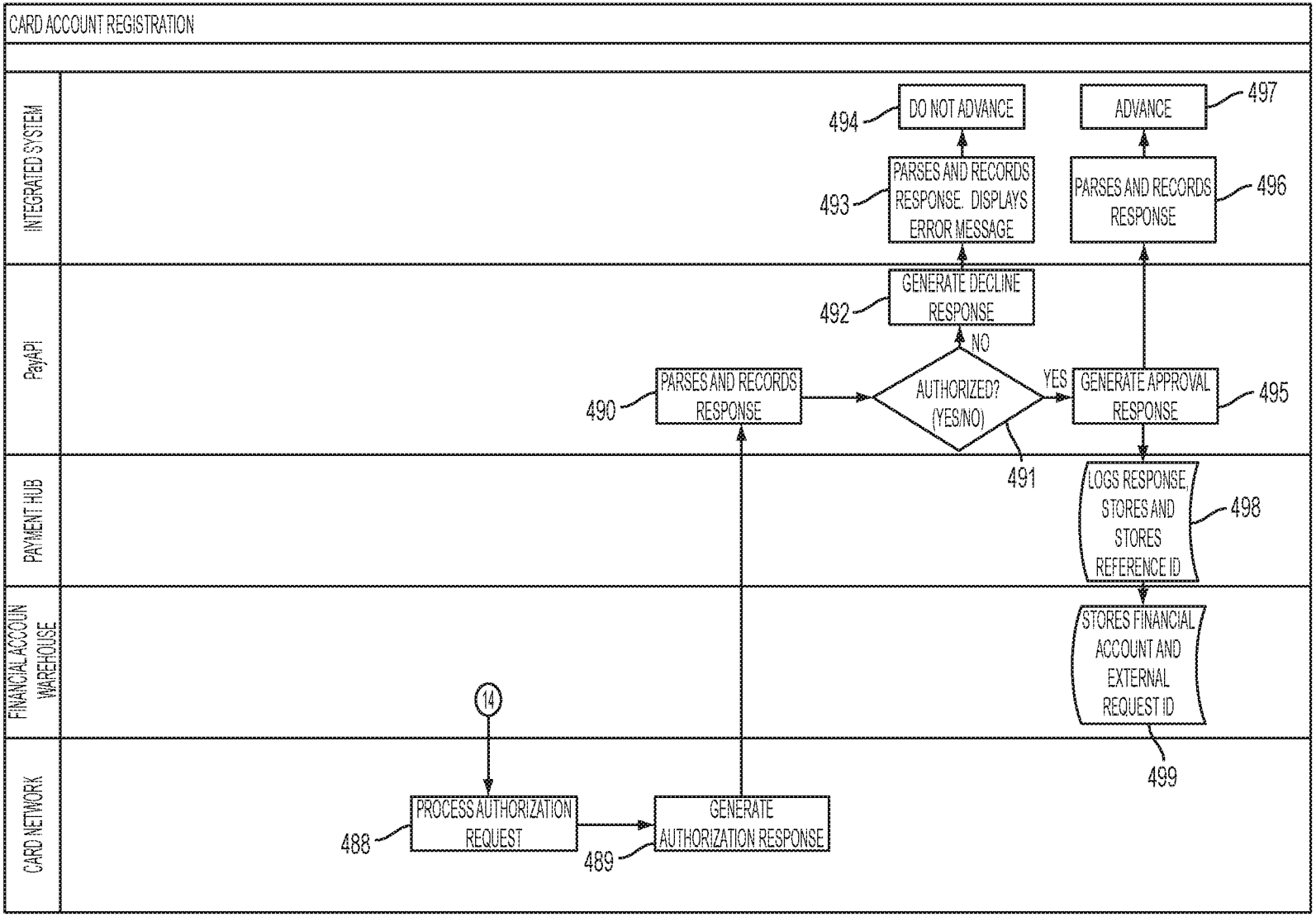

CARD ACCOUNT REGISTRATION
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
FINANCIAL ACCOUN WAREHOUSE
CARD NETWORK
494
DO NOT ADVANCE
497
ADVANCE
493
PARSES AND RECORDS RESPONSE. DISPLAYS ERROR MESSAGE
PARSES AND RECORDS RESPONSE
496
492
GENERATE DECLINE RESPONSE
NO
490
PARSES AND RECORDS RESPONSE
AUTHORIZED? (YES/NO)
YES
GENERATE APPROVAL RESPONSE
495
491
LOGS RESPONSE, STORES AND STORES REFERENCE ID
498
STORES FINANCIAL ACCOUNT AND EXTERNAL REQUEST ID
499
14
488
PROCESS AUTHORIZATION REQUEST
GENERATE AUTHORIZATION RESPONSE
489

FIG. 4j

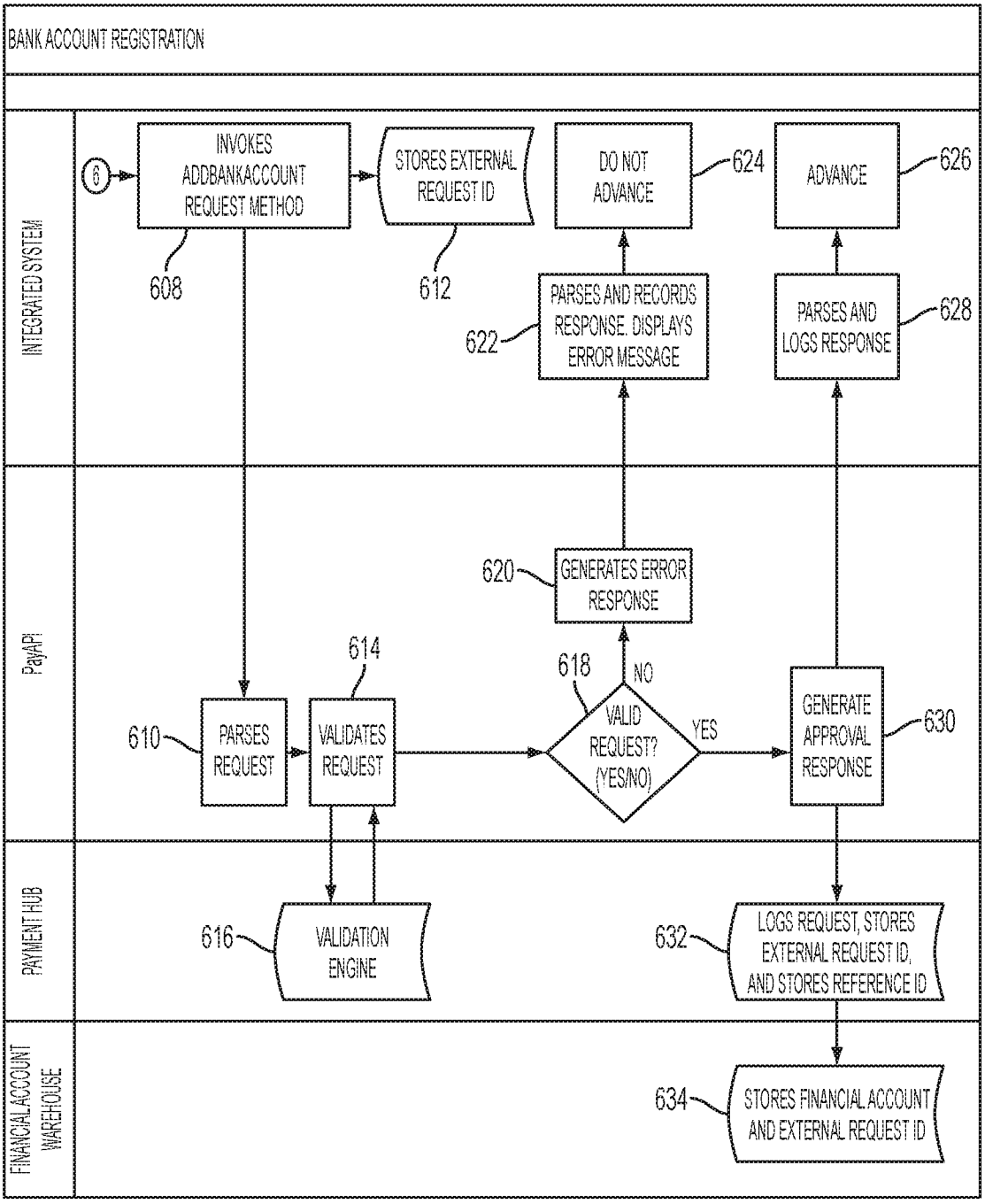

BANK ACCOUNT REGISTRATION
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
FINANCIAL ACCOUNT WAREHOUSE
INVOKES ADDBANKACCOUNT REQUEST METHOD
608
STORES EXTERNAL REQUEST ID
612
DO NOT ADVANCE
624
ADVANCE
626
PARSES AND RECORDS RESPONSE. DISPLAYS ERROR MESSAGE
622
PARSES AND LOGS RESPONSE
628
620
GENERATES ERROR RESPONSE
614
618
NO
610
PARSES REQUEST
VALIDATES REQUEST
VALID REQUEST? (YES/NO)
YES
GENERATE APPROVAL RESPONSE
630
616
VALIDATION ENGINE
632
LOGS REQUEST, STORES EXTERNAL REQUEST ID, AND STORES REFERENCE ID
634
STORES FINANCIAL ACCOUNT AND EXTERNAL REQUEST ID

FIG. 4k

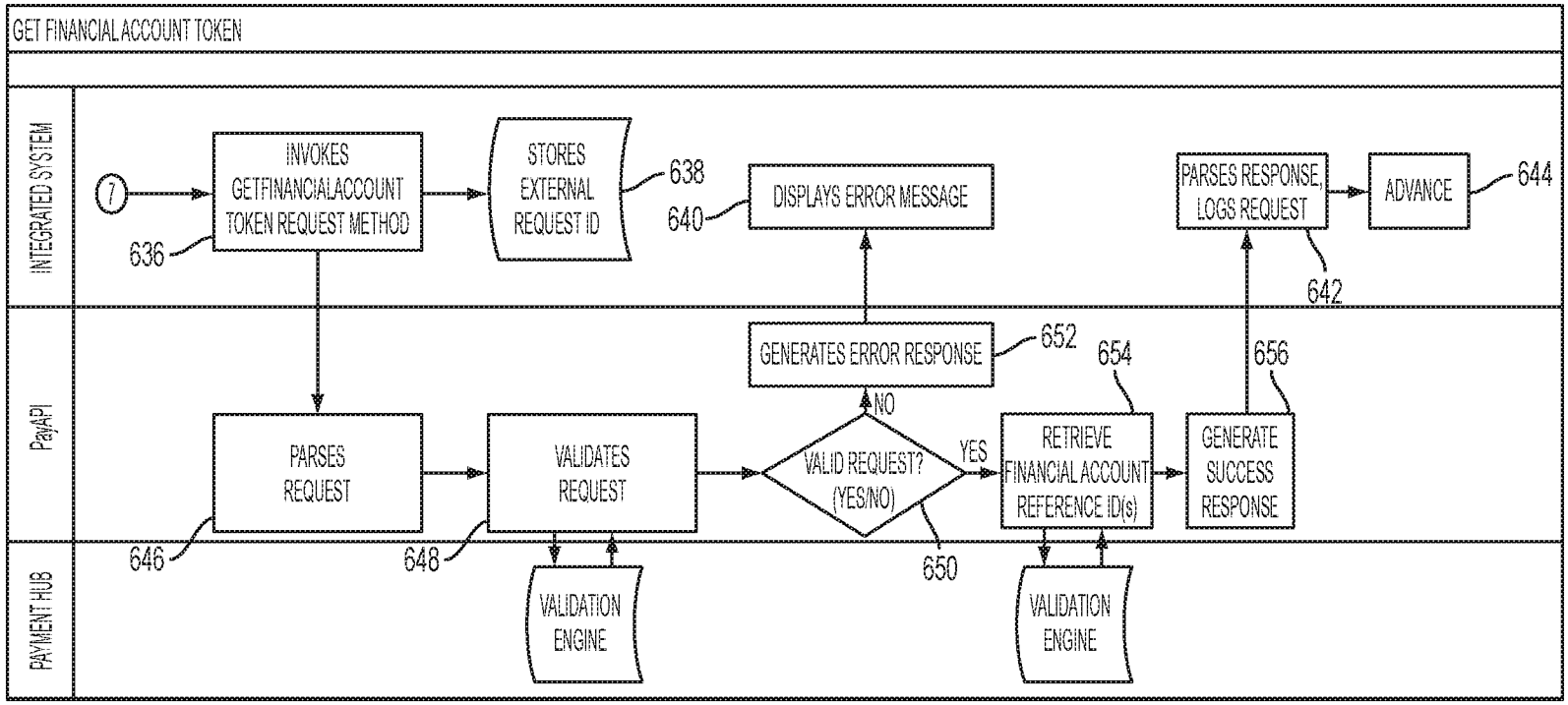

GET FINANCIAL ACCOUNT TOKEN
INTEGRATED SYSTEM
PayAPI
PAYMENT HUB
7
INVOKES GETFINANCIALACCOUNT TOKEN REQUEST METHOD
636
STORES EXTERNAL REQUEST ID
638
640
DISPLAYS ERROR MESSAGE
PARSES RESPONSE, LOGS REQUEST
642
ADVANCE
644
GENERATES ERROR RESPONSE
652
654
656
PARSES REQUEST
646
VALIDATES REQUEST
648
VALID REQUEST? (YES/NO)
NO
YES
650
RETRIEVE FINANCIAL ACCOUNT REFERENCE ID(s)
GENERATE SUCCESS RESPONSE
VALIDATION ENGINE
VALIDATION ENGINE

FIG. 4I

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR REGISTERING FINANCIAL ACCOUNTS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Robert Evan Pollin Date (Optional): 16 November 2012

Signature: Robert E. Pollin

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR REGISTERING FINANCIAL ACCOUNTS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

  filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Sean Allen Fleming Date (Optional): 16 November 2012

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHOD FOR REGISTERING FINANCIAL ACCOUNTS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT International application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Brian Edward Downey, Jr. Date (Optional): 16 November 2012

Signature: B Downey

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.