



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 3695	PAPER NUMBER
			NOTIFICATION DATE 10/05/2022	DELIVERY MODE 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

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and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.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 stored¹⁶ 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** 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. 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 802.11i 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.

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 networks⁵⁶ (including wireless network hardware with the dedicated chip⁷ required by the IEEE 802.11 standard⁵⁸ 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 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 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 webpage⁷⁶ at issue in DDR⁷⁷) 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."⁸⁰ Merchants were required to have specific retention requirements for all cardholder data⁸¹ 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 blocks⁸⁷ 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 masked⁸⁸ 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 necessary⁹⁵ 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 compromised⁹⁸ 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 unauthorized 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-l.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. (*Step 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

Art Unit: 3695

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.

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

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
Inventor/assignee, text/npl/foreign, bf-citation	09/28/2022	aa

/ABDULMAJEED AZIZ/ Primary Examiner, Art Unit 3695	
---	--

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

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/ABDULMAJEED AZIZ/ Primary Examiner, Art Unit 3695	
---	--

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	4	((("AUTOSCRIBE") near3 ("CORPORATION"))).A S,AANM.	(USPAT)	OR	ON	ON	2022/09/23 03:23 PM
L2	101	((("POLLIN") near3 ("Robert")) OR ((("DOWNEY") near3 ("Brian")) OR ((("FLEMING") near3 ("Sean"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2022/09/23 03:23 PM
L3	175	((("POLLIN") near3 ("Robert")) OR ((("DOWNEY") near3 ("Brian")) OR ((("FLEMING") near3 ("Sean"))).INV.	(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	2022/09/23 03:23 PM
L4	7	1	(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	2022/09/23 03:23 PM
L5	7	3 AND 4	(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,	OR	ON	ON	2022/09/23 03:23 PM

L6	8132	(enroll* register*) near10 (merchant vendor retailer) near3 (comput* server)	NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB) (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	2022/09/23 05:37 PM
L7	220	(enroll* register*) near10 (merchant vendor retailer) near3 (comput* server) AND (payer AND payee)	(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	2022/09/23 05:37 PM
L8	130	(enroll* register*) near10 (merchant vendor retailer) near3 (comput* server) AND token AND (payer AND payee)	(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	2022/09/23 05:38 PM
L9	71	(enroll* register*) near10 (merchant vendor retailer) near3	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY,	OR	ON	ON	2022/09/23 05:38 PM

L10	8	(comput* server) AND token AND (payer AND payee) AND stor* near5 token	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	2022/09/23 05:40 PM
L11	98	(enroll* register*) near10 (merchant vendor retailer) near3 (comput* server) AND token AND (payer AND payee) AND stor* near5 token AND @ad<"20120605"	(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	2022/09/23 05:41 PM
L12	22	(payer customer consumer payor) near10 (enroll* register*) near10 (merchant vendor retailer) near3 (comput* server) AND token AND stor* near5 token AND @ad<"20120605"	(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,	OR	ON	ON	2022/09/23 05:42 PM

L13	129	(payer customer consumer payor) near10 (enroll* register*) near10 (merchant vendor retailer) AND (token near3 (server vault)) AND @ad<"20120605"	TH, TN, TR, TW, UA, VN); FPRS; EPO; JPO; DERWENT; IBM_TDB) (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	2022/09/23 05:57 PM
L14	122	(payer customer consumer payor) near10 (enroll* register*) near10 (merchant vendor retailer) AND (token near3 (server vault)) AND @ad<"20120605" AND secure	(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	2022/09/23 05:57 PM
L15	66	(payer customer consumer payor) near10 (enroll* register*) near10 (merchant vendor retailer) AND (token near3 (server vault)) AND @ad<"20120605" AND secure near10 server	(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	2022/09/23 05:57 PM
L16	56	14 NOT 15	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA,	OR	ON	ON	2022/09/23 05:59 PM

L17	38	14 NOT 15	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	2022/09/23 06:02 PM
L18	167	(payer customer consumer payor) near10 (token near3 (server vault)) AND @ad<"20120605" AND secure near10 server	(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	2022/09/23 06:08 PM
L19	82	(payer customer consumer payor) near10 (token near3 (server vault)) AND @ad<"20120605" AND secure near10 server	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/23 06:08 PM
L20	18	(payer customer consumer payor) near10 (token near3 (server vault)) AND @ad<"20120605" AND secure near10 server AND (G06Q20/10 OR G06Q10/107 OR G06Q20/102 OR G06Q20/12 OR G06Q20/305 OR G06Q20/40 OR G06Q20/4014 OR G06Q10/00).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/23 06:09 PM
L21	1	"20100235286".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/23 06:13 PM
L22	3	((US-20120136796-A1 OR US-20110161233-A1 OR US-20100235286-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2022/09/23 06:27 PM

L23	45	(Artificial Intelligence) Similar to: 16/535,424 with 0 CPC Selections and 0 Text Selections Text: (US-20080147544-A1 OR US-20080147565- A1 OR WO- 2004021130-A9 OR US-7280981-B2 OR EP-1546956-A2 OR US-5677955-A OR CA- 2217593-A1 OR WO- 9631965-A1 OR EP- 0819345-A1 OR EP- 0819345-A4 OR US- 7711645-B2 OR US- 8010453-B2 OR WO- 2004021130-A2 OR JP- 2010507151-A OR EP- 1647952-A2 OR US- 20140279310-A1 OR JP-2002543541-A OR WO-2014152574-A1 OR US-7711621-B2 OR US-20080103985-A1 OR US-20040044621- A1 OR US-7571141-B2 OR US-20150006382- A1 OR JP-2003525478- A OR WO-03091959- A1 OR JP-H11503541- A OR CN-114819927-A OR US-8768840-B2 OR US-7941373-B1 OR US-20110106706-A1 OR US-7117171-B1 OR CA-2848299-A1 OR US-20140304149-A1 OR US-20110178923- A1 OR US- 20150193746-A1 OR US-8626652-B2 OR US-20070203833-A1 OR US-20140201079- A1 OR US- 20120330839-A1 OR US-20020169713-A1 OR US-20140310167- A1 OR US-7941368-B2 OR CN-1351738-A OR US-20150332272-A1 OR US-20120185316- A1 OR WO-03001866- A1 OR US- 20130117183-A1 OR US-8121945-B2 OR	(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))	OR	ON	ON	2022/09/23 06:37 PM
-----	----	---	---	----	----	----	------------------------

L24	3	US-8639623-B2 OR US-8452703-B2).did. ("20120259782" "20120030066").PN.	(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))	OR	ON	ON	2022/09/24 02:41 PM
L25	1	((US-20110161233- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2022/09/27 03:54 PM
L26	1	25 AND processor SAME customer	(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))	OR	ON	ON	2022/09/27 03:54 PM
L27	1	25 AND token SAME processor SAME merchant	(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))	OR	ON	ON	2022/09/27 04:52 PM
L28	1	25 AND (token vault) near10 customer	(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	2022/09/27 04:58 PM

L29	0	(payer customer consumer payor) near3 device SAME internet near10 (payment transaction secure) near3 server AND (token near3 (server vault)) AND @ad<"20120605" AND (G06Q20/10 OR G06Q10/107 OR G06Q20/102 OR G06Q20/12 OR G06Q20/305 OR G06Q20/40 OR G06Q20/4014 OR G06Q10/00).cpc.	NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO)) (US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 06:06 PM
L30	3	(payer customer consumer payor) near3 device SAME internet near10 (payment transaction secure) near3 server AND (token near3 (server vault)) AND @ad<"20120605"	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 06:06 PM
L31	31	(payer customer consumer payor) near3 device SAME internet near10 server AND (token near3 (server vault)) AND @ad<"20120605"	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 06:07 PM
L32	10	(payer customer consumer payor) near3 device SAME internet near10 server AND (token near3 (server vault)) AND @ad<"20120605" AND secure near10 server	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 06:08 PM
L33	308	payee near10 payment SAME amount AND @ad<"20120605" AND secure near10 server	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 10:07 PM
L34	34	payee near10 payment SAME amount AND @ad<"20120605" AND secure near10 server near10 internet	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27 10:08 PM
L35	6	payer near10 payee	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/27

L36	45	near10 payment SAME amount AND @ad<"20120605" AND secure near10 server near10 internet (Artificial Intelligence) Similar to: 16/535,424 with 0 CPC Selections and 0 Text Selections Text: (US-20080147544-A1 OR US-20080147565-A1 OR WO-2004021130-A9 OR US-7280981-B2 OR EP-1546956-A2 OR US-5677955-A OR CA-2217593-A1 OR WO-9631965-A1 OR EP-0819345-A1 OR EP-0819345-A4 OR US-7711645-B2 OR US-8010453-B2 OR WO-2004021130-A2 OR JP-2010507151-A OR EP-1647952-A2 OR US-20140279310-A1 OR JP-2002543541-A OR WO-2014152574-A1 OR US-7711621-B2 OR US-20080103985-A1 OR US-20040044621-A1 OR US-7571141-B2 OR US-20150006382-A1 OR JP-2003525478-A OR WO-03091959-A1 OR JP-H11503541-A OR CN-114819927-A OR US-8768840-B2 OR US-7941373-B1 OR US-20110106706-A1 OR US-7117171-B1 OR CA-2848299-A1 OR US-20140304149-A1 OR US-20110178923-A1 OR US-20150193746-A1 OR US-8626652-B2 OR US-20070203833-A1 OR US-20140201079-A1 OR US-20120330839-A1 OR US-20020169713-A1 OR US-20140310167-A1 OR US-7941368-B2 OR CN-1351738-A OR	(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))	OR	ON	ON	10:10 PM 2022/09/28 06:01 PM
-----	----	--	--	----	----	----	--

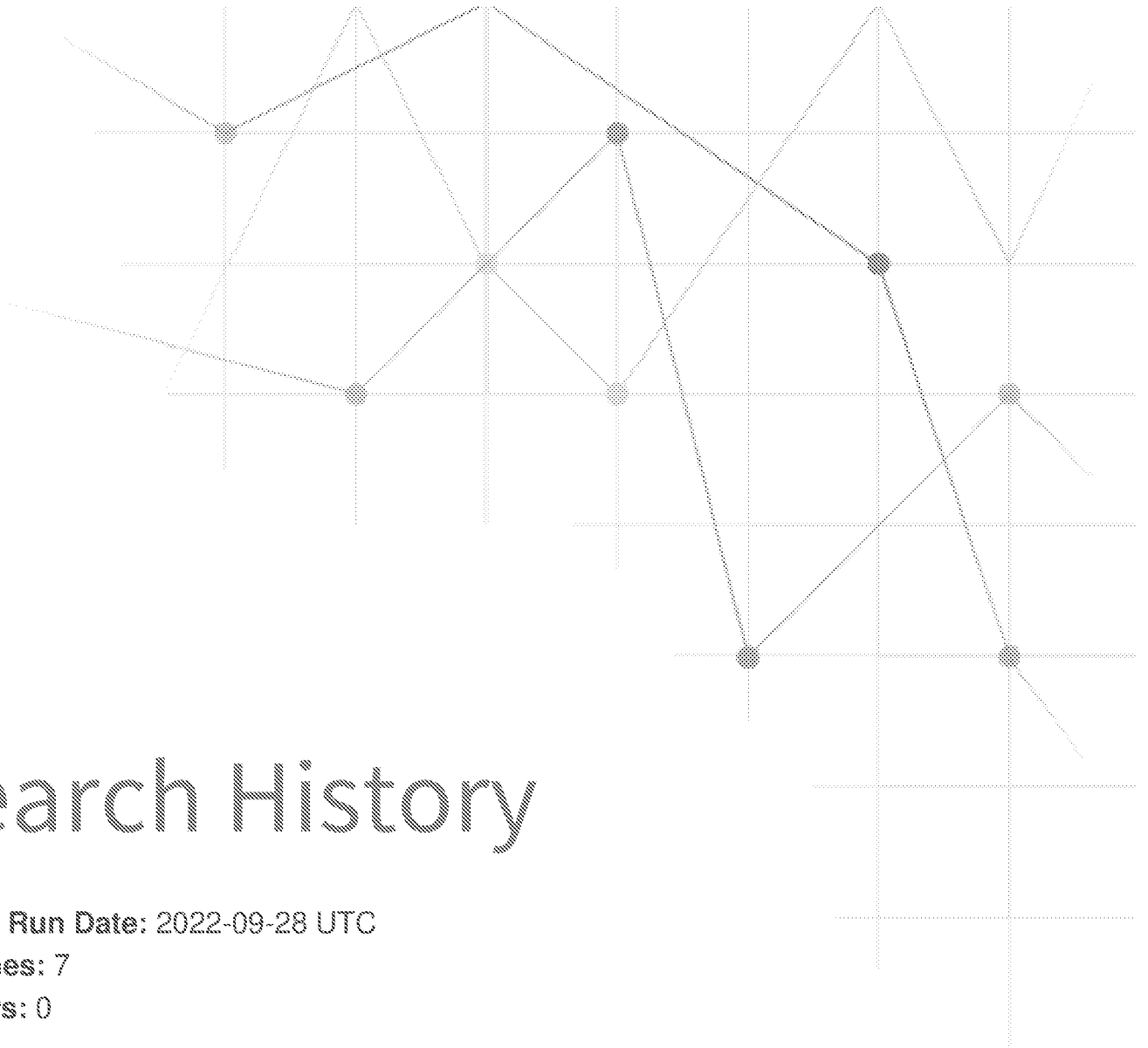
L37	490	US-20150332272-A1 OR US-20120185316-A1 OR WO-03001866-A1 OR US-20130117183-A1 OR US-8121945-B2 OR US-8639623-B2 OR US-8452703-B2).did. ("2012/0136796" "2012/0030066" "2011/0161233" "2010/0235286" "2004/0148252" "2012/0259782").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:02 PM
L38	94	37 AND @ad<"20120605"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:02 PM
L39	18	37 AND @ad<"20120605" AND (merchant vendor retailer) near3 server	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:02 PM
L40	11	37 AND @ad<"20120605" AND (merchant vendor retailer) near3 server AND token*	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:03 PM
L41	9	37 AND @ad<"20120605" AND (merchant vendor retailer) near3 server AND token* AND payment near3 (server processor)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:03 PM
L42	6	37 AND @ad<"20120605" AND (merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device)	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2022/09/28 06:04 PM
L43	51	(merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server AND PCI AND @ad<"20120605"	(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,	OR	ON	ON	2022/09/28 06:11 PM

L44	5	(merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server AND PCI SAME merchant AND @ad<"20120605"	TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB) (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	2022/09/28 06:12 PM
L45	17	(merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server AND PCI SAME secure AND @ad<"20120605"	(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	2022/09/28 06:12 PM
L46	0	(merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server AND PCI SAME secure AND @ad<"20120605" NOT wallet	(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	2022/09/28 06:13 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
-------	------	--------------	-----	------------------	---------	---------------------	------------

N1	66	((merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/28 06:07 PM
N2	24	((merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/28 06:07 PM
N3	7	((merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/28 06:07 PM
N4	3	((merchant vendor retailer) near3 server AND token* AND payment near3 (server processor) AND (consumer customer) near3 (computer device) AND secure near3 server).clm. AND @ad<"20120605"	(US-PGPUB; USPAT)	OR	ON	ON	2022/09/28 06:08 PM



Search History

Report Run Date: 2022-09-28 UTC

Searches: 7

Markers: 0

Search #	Timestamp	Results	Page
1	2022-09-23 21:44 UTC	3,442,194	3
2	2022-09-23 21:45 UTC	1,121,666	3
3	2022-09-23 21:45 UTC	22,320,635	4
4	2022-09-23 21:53 UTC	22,320,635	5
5	2022-09-23 21:54 UTC	10,160,433	5
6	2022-09-23 22:11 UTC	36,402	5
7	2022-09-23 22:12 UTC	3159	5



Content: Non-Patent Literature (23)

IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | IEEE Xplore Publications: SMPTE Periodicals | IEEE Xplore Publications: SMPTE Conferences | IEEE Xplore Publications: SMPTE Standards | IEEE Xplore Publications: MIT Press eBooks | IEEE Xplore Publications: Wiley-IEEE eBooks | IEEE Xplore Publications: IBM Periodicals | IEEE Xplore Publications: URSI Periodicals | IEEE Xplore Publications: VDE Conferences | IEEE Xplore Publications: Periodicals from China | IP.com Prior Art Database: The IP.com Journal | IP.com Prior Art Database: Internet Society RFC | IP.com Prior Art Database: IBM TDB Archive | IP.com Prior Art Database: Legacy Journals | IP.com Prior Art Database: Software Patent Institute | OnePetro.org: Periodicals at OnePetro.org | OnePetro.org: Conferences at OnePetro.org | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 2022-09-23 21:44 UTC | 3,442,194 results from

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Text

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.

Concept Modifiers: None

Filters: None

2 2022-09-23 21:45 UTC | 1,121,666 results from

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Same as Search 1

Concept Modifiers: None

Filters (1):

Publication Date: To 2012-06-05



Content: Patent Publications (167)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic

Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Jordan Applications | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Saudi Arabia Applications | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Patents | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications

3 2022-09-23 21:45 UTC | 22,320,635 results from 

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Text

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.

Concept Modifiers: None

Filters: None

4 2022-09-23 21:53 UTC | 22,320,635 results from 

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Text

receiving, at a merchant server, enrollment data identifying a payer; receive financial account information provided by the payer at a secure server; generating a token by the secure server representing financial account information received by the secure server, wherein the merchant server only receives the token and the token is not provided to the payer; storing the token with the payer enrollment data; and processing a payment from the payer using the token via a payment processor.

Concept Modifiers: None

Filters: None

5 2022-09-23 21:54 UTC | 10,160,433 results from 

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Same as Search 4

Concept Modifiers: None

Filters (1):

Application Date: To 2012-06-05

6 2022-09-23 22:11 UTC | 36,402 results from 

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Text

the secure server does not provide the electronic data token to the payer

Concept Modifiers: None

Filters: Same as Search 5

7 2022-09-23 22:12 UTC | 3159 results from 

De-Dup: None | Cut-off: None | Sort: Relevance

Main Concept: Text

server does not send the token to the payer

Concept Modifiers: None

Filters: Same as Search 5

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: RCEX

Doc description: Request for Continued Examination (RCE)

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

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

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 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 - 1 month with \$0 paid	2251	1	110	110
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	680	680
Total in USD (\$)				790

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	no	3
			cb8ee561a191092f800187e6cab31b603644d975		

Warnings:

Information:

2	Amendment Submitted/Entered with Filing of Continued Prosecution Application (CPA)/Request for Continued Examination(RCE)	20220411_Response_RCE.pdf	208861	no	28
			579218e0d10882b5cb3bd41b87196bdb618d25d3		

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	40791	no	2
			3764dfcce933800445809ab3f173adacb84dd70d		

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 ~~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 idea¹ 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 2A² 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 steps⁷ and/or adding additional nodes to a prior art system⁸ – 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 steps⁹ – 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 application¹² 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 stored¹⁶ 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 URL⁴⁹ or a widget or window within a website provided by the merchant server⁵⁰), 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 networks⁵⁶ (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 chip⁵⁷ required by the IEEE 802.11i standard⁵⁸ 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 webpage⁷⁶ 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 data⁸¹ 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 blocks⁸⁷ 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 masked⁸⁸ 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 necessary⁹⁵ 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 ciphertext 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 compromised⁹⁸ 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 unauthorized 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

<i>Applicant-Initiated Interview Summary</i>	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.

<i>Applicant-Initiated Interview Summary</i>	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

124452.00122/126639850v.2

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 method¹ 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 method² 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 be 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 categories¹¹ 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 3697	PAPER NUMBER
			NOTIFICATION DATE 12/10/2021	DELIVERY MODE 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

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 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”. 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.

<i>Notice of References Cited</i>	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.

<i>Search Notes</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN, Robert Evan
	Examiner PIERRE L MACCAGNO	Art Unit 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	
--	--

<i>Search Notes</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN, Robert Evan
	Examiner PIERRE L MACCAGNO	Art Unit 3697

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PIERRE L MACCAGNO/ Examiner, Art Unit 3697	
--	--

<i>Index of Claims</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.
	Examiner PIERRE L MACCAGNO	Art Unit 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			✓							

<i>Index of Claims</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.
	Examiner PIERRE L MACCAGNO	Art Unit 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").URP N.	(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

L11	28	token ((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

L23	5	@py<"2013" ((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

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"	JPO; DERWENT; IBM_TDB) (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

L32	23	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)	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 (G06Q20/102).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 11:52 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.	

**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.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	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

NON-PATENT LITERATURE DOCUMENTS

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

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.

**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 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.

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: 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.

124452.00122/126639850v.2

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~~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 payer~~~~claim 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 server~~~~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. (Currently Amended): The method of claim 8, wherein ~~the secure connection is a widget or window within a website provided by the merchant server~~~~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. (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 server~~~~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. (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 be 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 categories³ 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	yes	23
			a8c265e6f103200fb86a477f45bcefac69749e85		
	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	no	2
			ba52f240beb1617ca37ceaddee7067abb20265e43		
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 3696	PAPER NUMBER
			NOTIFICATION DATE 03/17/2021	DELIVERY MODE 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

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	Viiidu; 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.

<i>Index of Claims</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.
	Examiner PIERRE L MACCAGNO	Art Unit 3696

✓	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								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								

<i>Search Notes</i> 	Application/Control No. 16/535,424	Applicant(s)/Patent Under Reexamination POLLIN et al.
	Examiner PIERRE L MACCAGNO	Art Unit 3696

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/10	03/12/2021	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

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/PIERRE L MACCAGNO/ Examiner, Art Unit 3696	
--	--

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.	

**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.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	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

NON-PATENT LITERATURE DOCUMENTS

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

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.

**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 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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	12	autoscribe.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/10 21:49
S2	10	autoscribe.as. and (pollin).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/10 21:54
S3	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	2021/03/10 21:59
S4	4,147	payment with process\$3 with transaction with first with second	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 06:43
S5	201	payment with process\$3 with transaction with first with second with token	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 06:44
S6	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	2021/03/11 06:45
S7	45	(payment with transaction with first with second with token)and (G06Q20/10).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO;	OR	ON	2021/03/11 06:49

			JPO; DERWENT			
S8	49	("2011/0029416").URPN.	USPAT	OR	ON	2021/03/11 07:00
S9	2	(aaron same greenspan).IN.	USPAT	OR	ON	2021/03/11 07:02
S10	272	(payment with process\$3 with transaction with first with second)same token	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 07:05
S11	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	2021/03/11 07:06
S12	60	((payment with transaction with first with second) same token)and (G06Q20/10).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 07:12
S13	138	((payment with first with second) same token)and (G06Q20/10).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 07:44
S14	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	2021/03/11 07:53
S15	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	2021/03/11 07:54
S16	830	(payment with process\$3 with transaction with first with second) and @py<="2012"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 07:57

S17	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	2021/03/11 07:58
S18	426	(payment with transaction with first with second) and token and @py<="2012"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 08:00
S19	1,689	(payment with first with second) and token and @py<="2012"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/11 08:00
S20	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	2021/03/11 08:01
S21	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	2021/03/11 08:13
S22	427	((payment) with token)and (G06Q20/10).CPC. and @py<"2013"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/12 13:18
S23	5	((payment) with (data adj token))and (G06Q20/10).CPC. and @py<"2013"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT	OR	ON	2021/03/12 14:10
S24	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	2021/03/12 14:13

3/12/2021 7:34:38 PM
C:\Users\pmaccagno\Documents\EAST\Workspaces\16535424.wsp

Dialog

STIC
Scientific and Technical
Information Center

Search Strategy from Dialog

March 12 2021 19:33

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, Current Contents® Search, Derwent Drug File, Derwent Drug Registry, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, EconLit, Ei Compendex®, Ei EnCompassLIT, Embase®, EMCare®, ERIC, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE, GeoRef, Global Health, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Material Safety Datasheets -OHS™, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geostrophysical Abstracts, Morressier Life Science Conference Abstracts and Posters, New England Journal of Medicine, Northern Light Life Sciences Conference Abstracts, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Dissertations and Theses Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prous Science Daily Essentials, Prous Science Drug Data Report, Prous Science Drugs Of The Future™, Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record

Set#	Searched for	Results
S1	(((((payment near/15 process[*3]) near/15 transaction) near/15 first) near/15 second) near/15 token	10°
S2	(((((payment near/15 process[*3]) near/15 transaction) near/15 first) near/15 second) near/40 token	11°
S3	((payment) near/15 ((data or transaction) pre/0 token))	104°

° Duplicates are removed from the search and from the result count.

Contact ProQuest

Copyright © 2021 ProQuest LLC. All rights reserved. - **Terms and Conditions**



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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/535,424	08/08/2019	Robert Evan POLLIN	124452.00122

CONFIRMATION NO. 2047

PUBLICATION NOTICE



OC000000112994535

27557
BLANK ROME LLP
1825 Eye Street NW
WASHINGTON, DC 20006-5403

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

Publication No.US-2019-0362324-A1

Publication Date:11/28/2019

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/535,424				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	75		N/A				
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	330		N/A				
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	380		N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	25	minus 20 = 5	x 50 =	250	OR					
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x 230 =	0.00						
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).			0.00						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00						
			TOTAL	1035		TOTAL				
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=	OR	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=	OR	x	=
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** 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 found in the appropriate box in column 1.										



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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/535,424	08/08/2019	3693	1035	124452.00122	25	3

CONFIRMATION NO. 2047

FILING RECEIPT



27557
BLANK ROME LLP
1825 Eye Street NW
WASHINGTON, DC 20006-5403
UNITED STATES OF AMERICA

Date Mailed: 08/21/2019

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

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

Applicant(s)

Autoscribe Corporation, Gaithersburg, MD;

Power of Attorney: The patent practitioners associated with Customer Number 27557

Domestic Priority data as claimed by applicant

This application is a CON of 15/408,185 01/17/2017
which is a CON of 13/679,545 11/16/2012 PAT 9576279
which claims benefit of 61/655,482 06/05/2012
and claims benefit of 61/698,574 09/08/2012

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 08/19/2019

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/535,424**

Projected Publication Date: 11/28/2019

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

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

Preliminary Class

705

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

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 U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

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.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	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.

NON-PATENT LITERATURE DOCUMENTS

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.

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 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 Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
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/Judy Yeddo		
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:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	75	75
UTILITY SEARCH FEE	2111	1	330	330
UTILITY EXAMINATION FEE	2311	1	380	380
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2202	5	50	250
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1035

Electronic Acknowledgement Receipt	
EFS ID:	36820565
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/Judy Yeddo
Filer Authorized By:	Michael C. Greenbaum
Attorney Docket Number:	124452.00122
Receipt Date:	08-AUG-2019
Filing Date:	
Time Stamp:	13:14:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 1035
RAM confirmation Number	E201988D14361098
Deposit Account	232185
Authorized User	Judy Yeddo
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	Transmittal.pdf	197258	no	2
			ffe9dd6b0686b53ce1799932450643be6e596c77		
Warnings:					
Information:					
2	Application Data Sheet	ADS.pdf	1064054	no	6
			58bdc784e6f0752f5b48ea9613a566f25185e9d6		
Warnings:					
Information:					
3		Specification.pdf	123815	yes	30
			91c36fcb81cd5582be8c518c04a085ab3976b2f9		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	23	
	Claims		24	29	
	Abstract		30	30	
Warnings:					
Information:					
4	Drawings-only black and white line drawings	Figures.pdf	121245	no	15
			f6118d56c7c2dd53503fed2652f03bc462754cfe		
Warnings:					
Information:					
5	Oath or Declaration filed	Declaration.pdf	645728	no	3
			b3b491e66f0b09d2ec23486562bb3949ad3ed619		

Warnings:					
Information:					
6	Power of Attorney	POA.pdf	181616	no	1
			5d847854ace67e69d4eba6a5f8aaf649669f507d		
Warnings:					
Information:					
7	Transmittal Letter	IDS.pdf	20421	no	2
			ccc2c4f540c25251cd30ee658a318c603f1838b8		
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Form (SB08)	SB08.pdf	1034852	no	5
			881840b0c13b62d95eda019f6d335f908892a64		
Warnings:					
Information:					
9	Fee Worksheet (SB06)	fee-info.pdf	36801	no	2
			40e5eff6e6e81d54c820ff8bac769b343c3793bc		
Warnings:					
Information:					
Total Files Size (in bytes):			3425790		
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. <u>New Applications Under 35 U.S.C. 111</u> 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. <u>National Stage of an International Application under 35 U.S.C. 371</u> 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. <u>New International Application Filed with the USPTO as a Receiving Office</u> 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.					

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:
- 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.)

27557

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)

5/21/2017

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.

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

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 <i>(Only for new nonprovisional applications under 37 CFR 1.53(b))</i>		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 <i>See MPEP chapter 600 concerning utility patent application contents.</i>	ADDRESS TO: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450																
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	ACCOMPANYING APPLICATION PAPERS 10. ☐ Assignment Papers (cover sheet & document(s)) Name of Assignee _____ 11. ☐ 37 CFR 3.73(c) Statement ☒ Power of Attorney (when there is an assignee) 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																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">Name</td> <td colspan="2"></td> </tr> <tr> <td colspan="2">Address</td> <td colspan="2"></td> </tr> <tr> <td>City</td> <td>State</td> <td>Zip Code</td> <td></td> </tr> <tr> <td>Country</td> <td>Telephone</td> <td>Email</td> <td></td> </tr> </table>		Name				Address				City	State	Zip Code		Country	Telephone	Email	
Name																	
Address																	
City	State	Zip Code															
Country	Telephone	Email															
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Signature</td> <td>/Michael C. Greenbaum/</td> <td>Date</td> <td>August 8, 2019</td> </tr> <tr> <td>Name (Print/Type)</td> <td>Michael C. Greenbaum</td> <td>Registration No. (Attorney/Agent)</td> <td>28,419</td> </tr> </table>		Signature	/Michael C. Greenbaum/	Date	August 8, 2019	Name (Print/Type)	Michael C. Greenbaum	Registration No. (Attorney/Agent)	28,419								
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	Rockville	State/Province	MD	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	1045 Wintergreen Terrace					
Address 2						
City	Rockville	State/Province	MD			
Postal Code	20850	Country i	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	Alexandria	State/Province	VA	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	6133 Wellington Commons Drive					
Address 2						
City	Alexandria	State/Province	VA			
Postal Code	22310	Country i	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 i	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 ¹	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

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	Gaithersburg	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:

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 (designated 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 (designated 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.

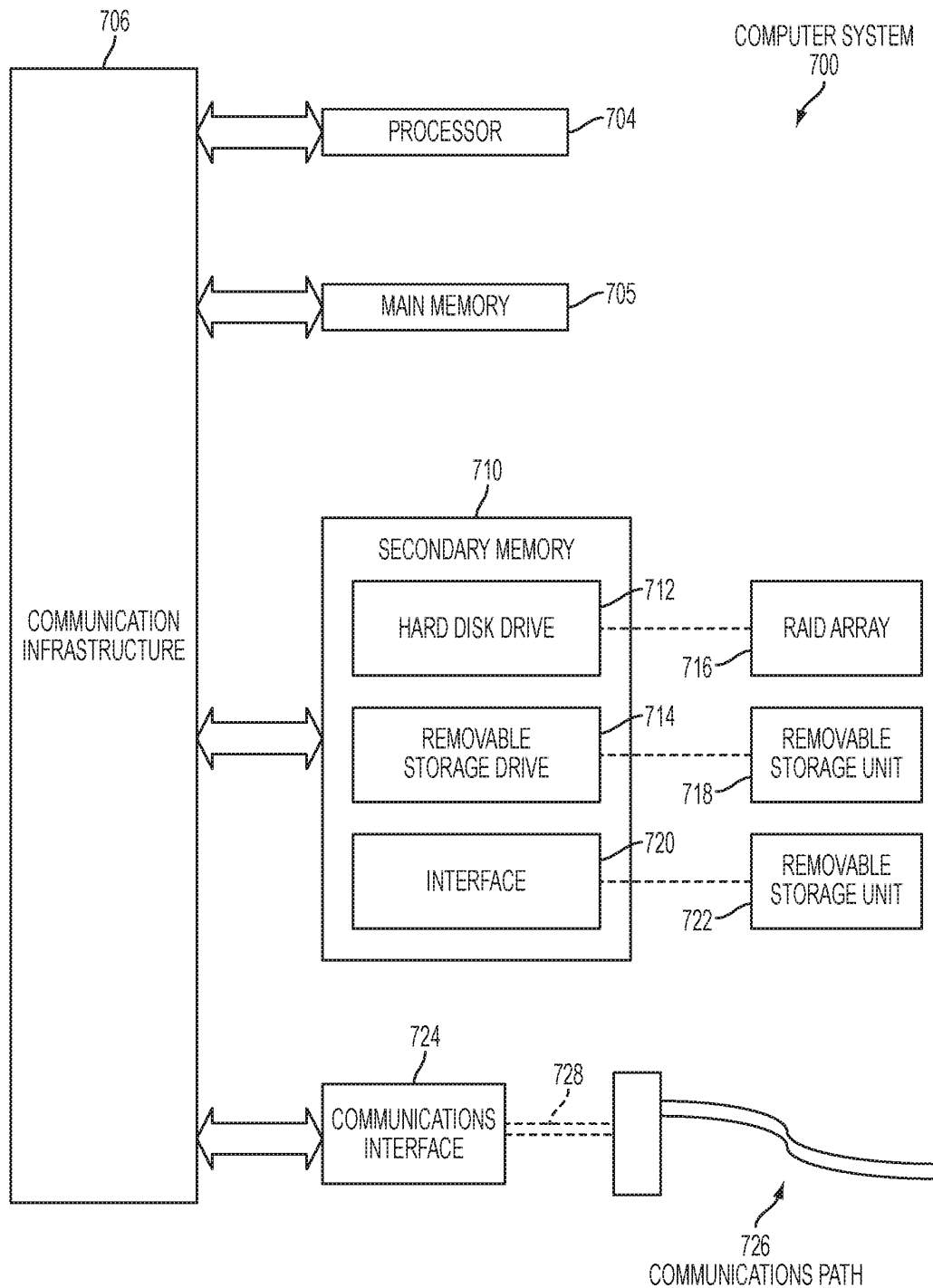


FIG. 1

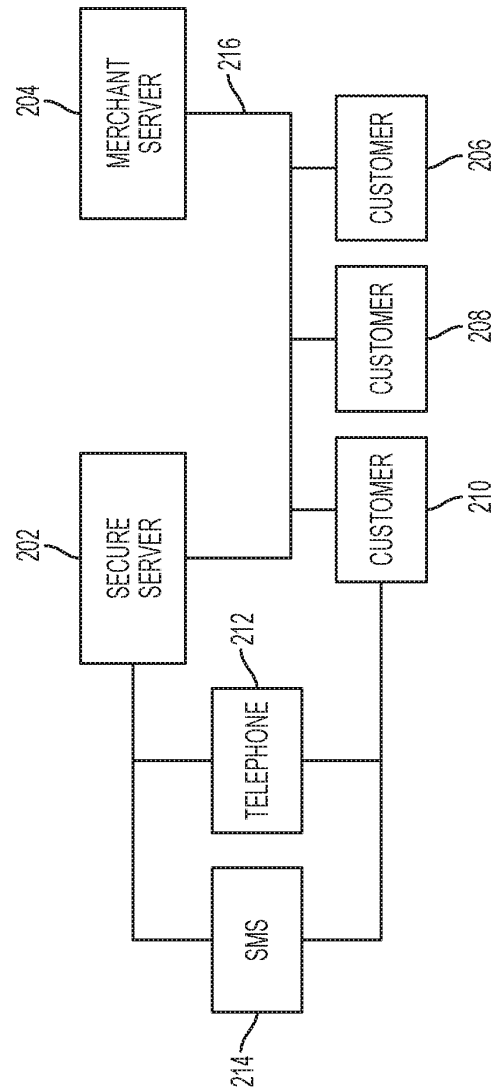


FIG. 2

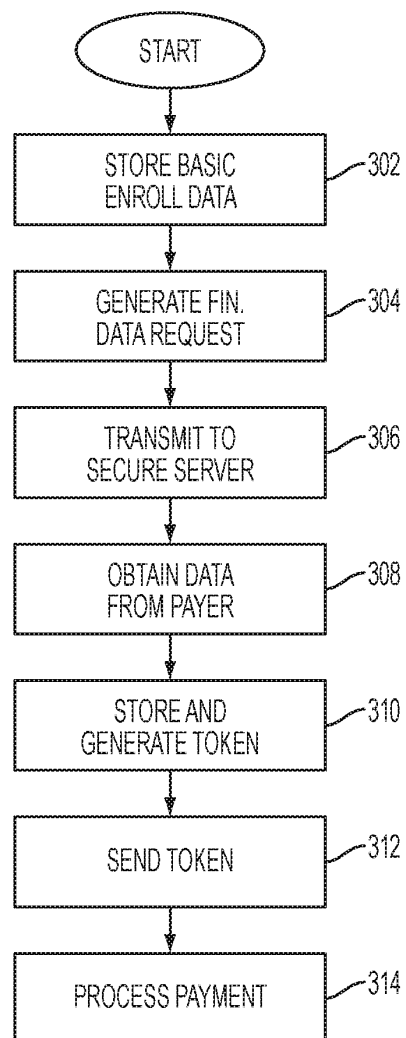


FIG. 3

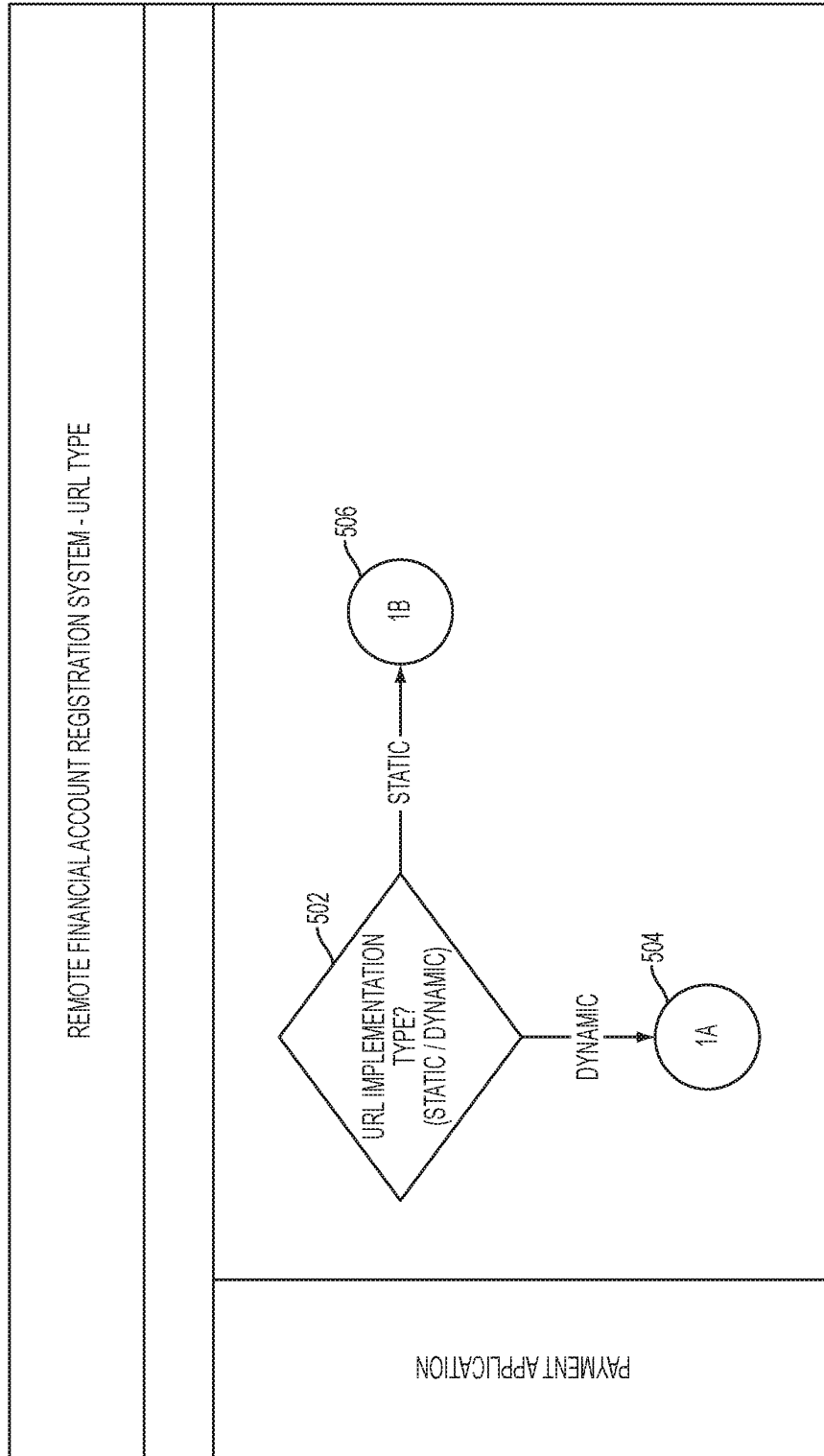
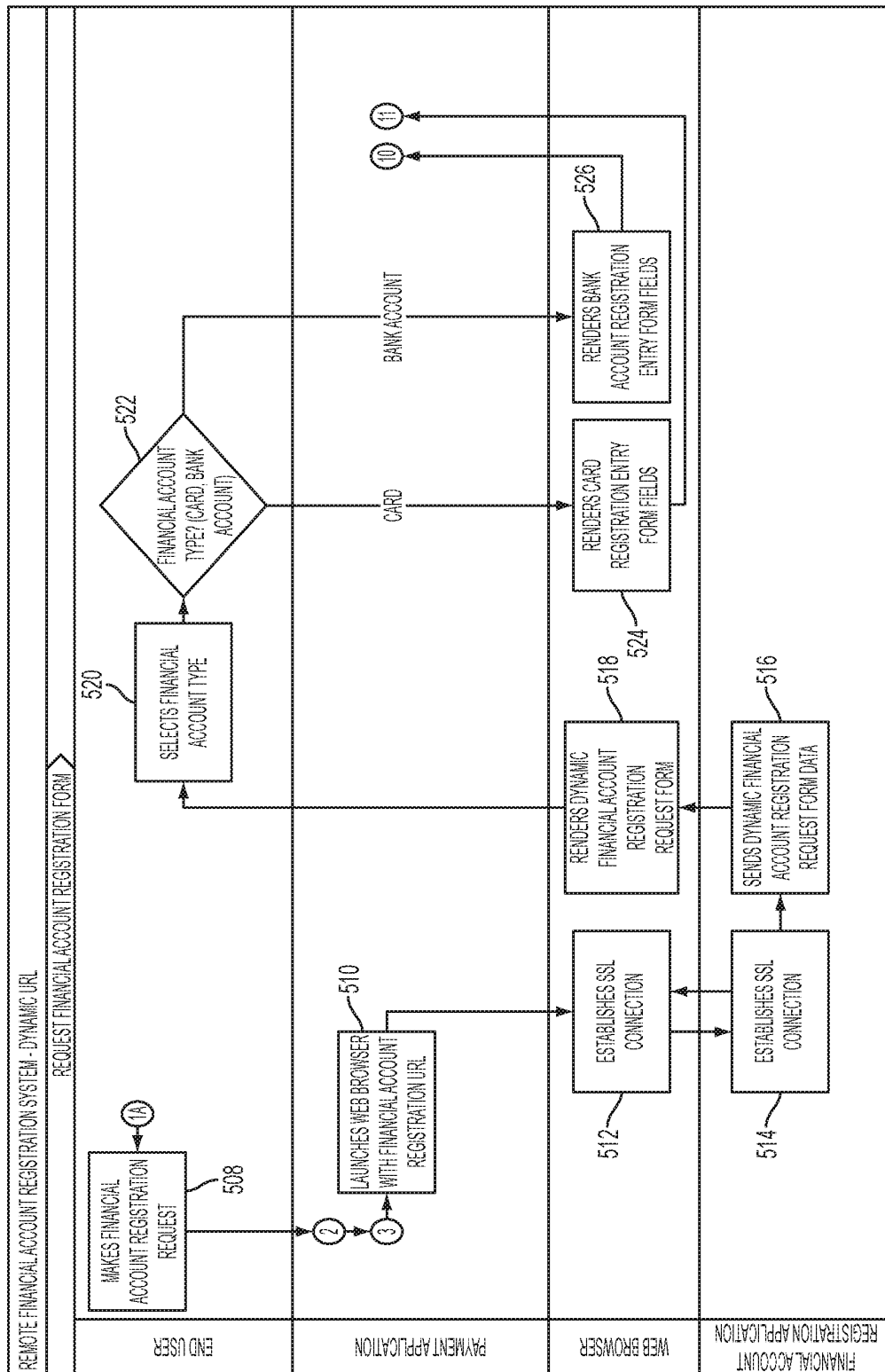


FIG. 4a



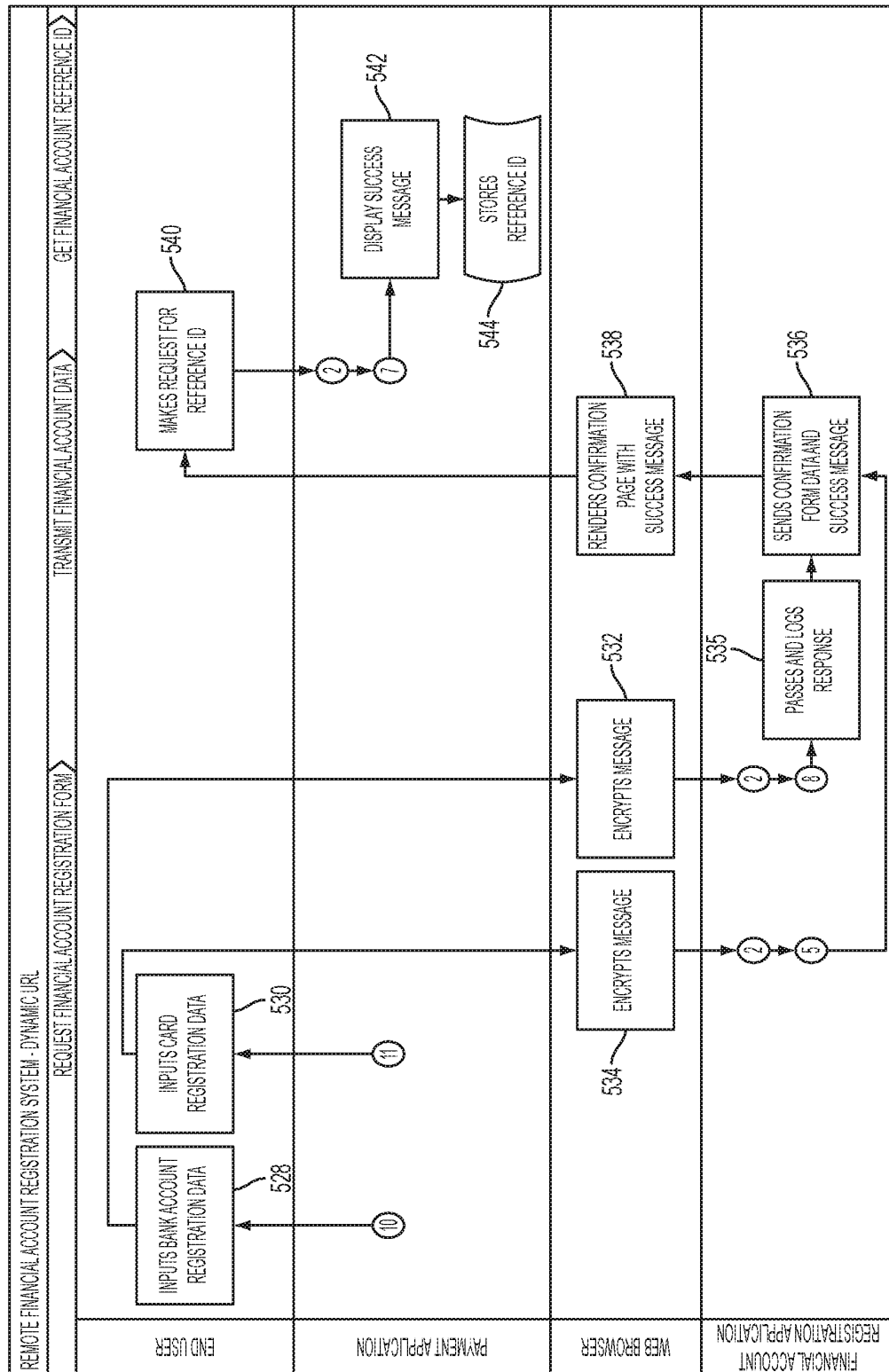


FIG. 4c

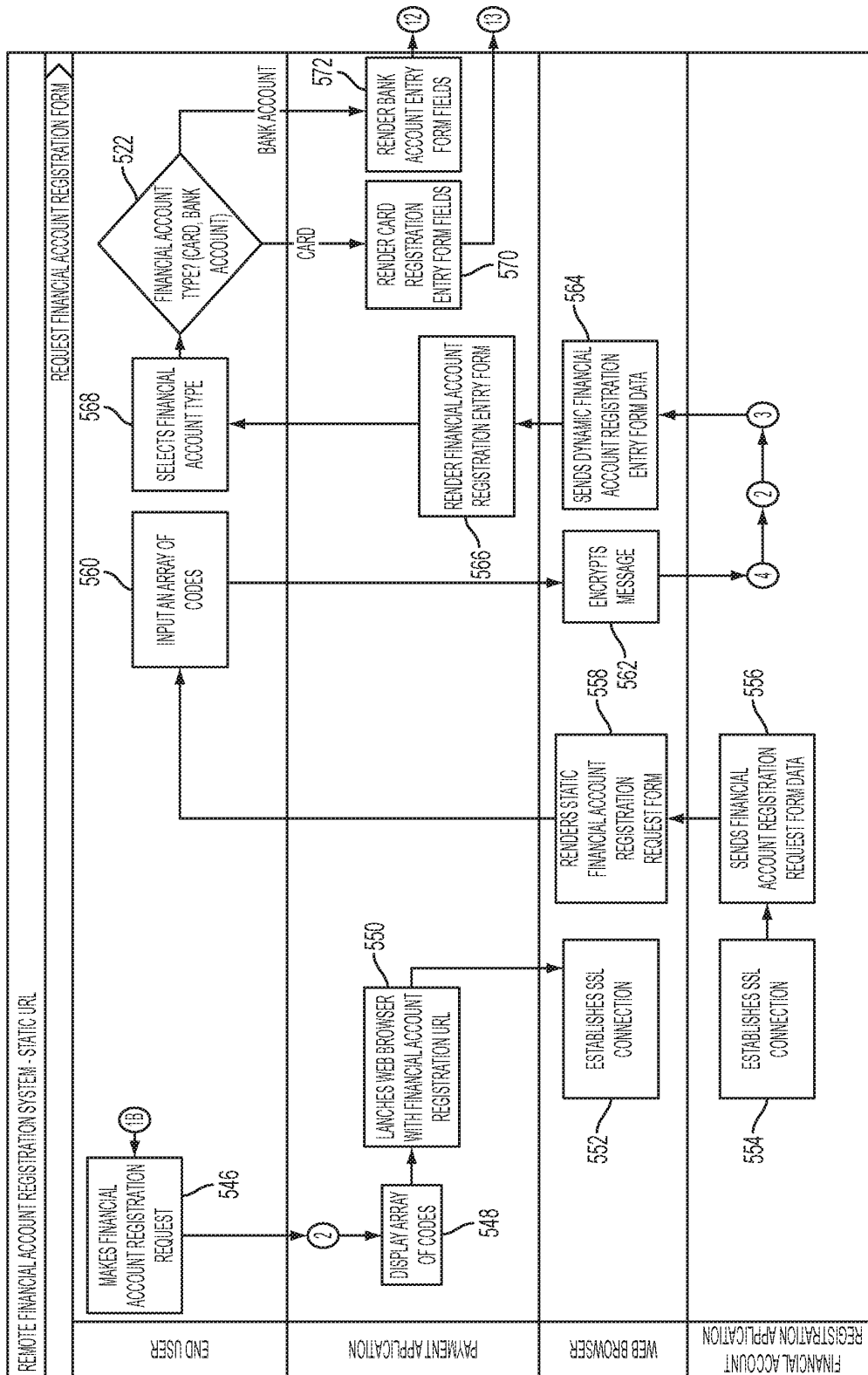


FIG. 4d

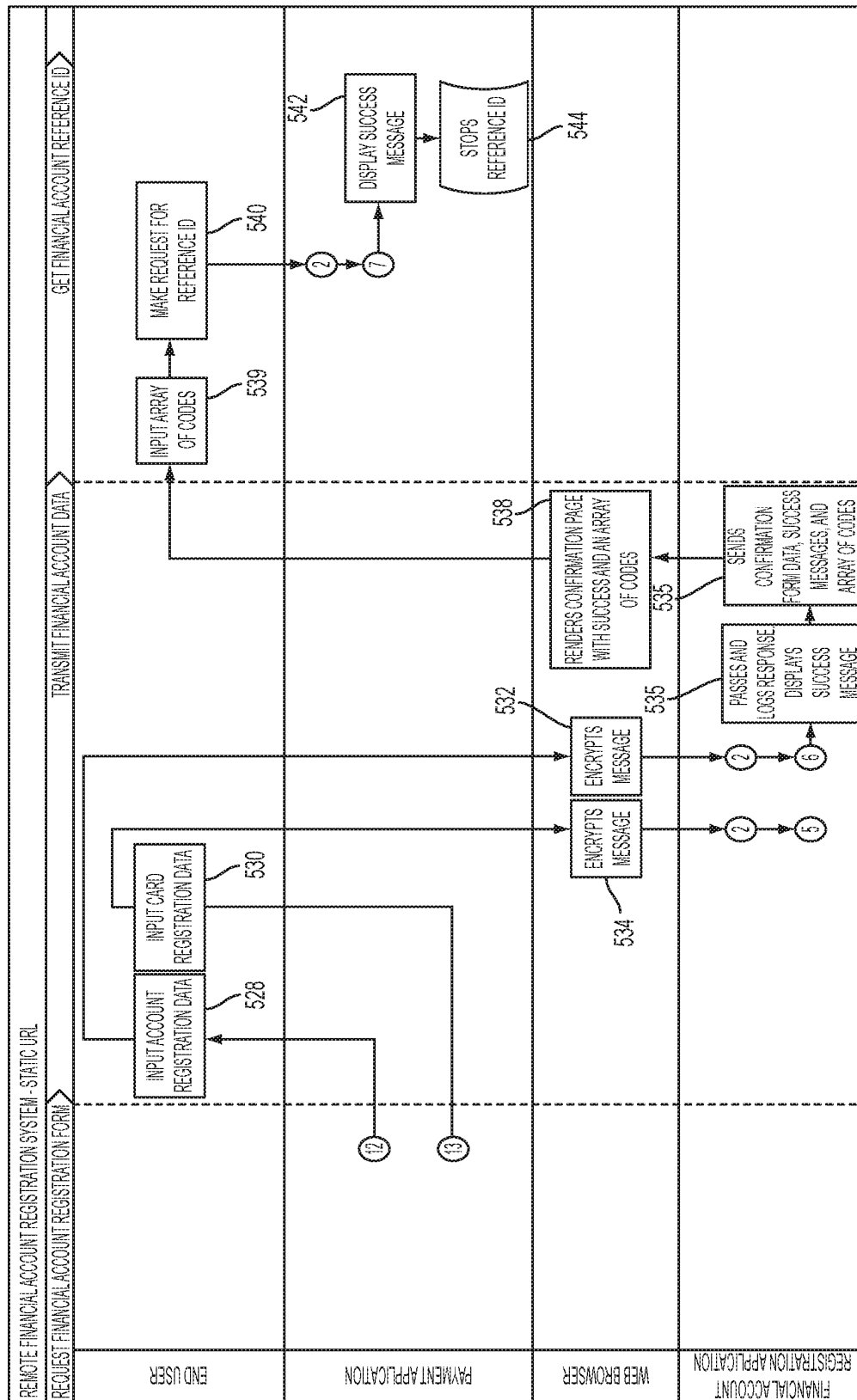


FIG. 4e

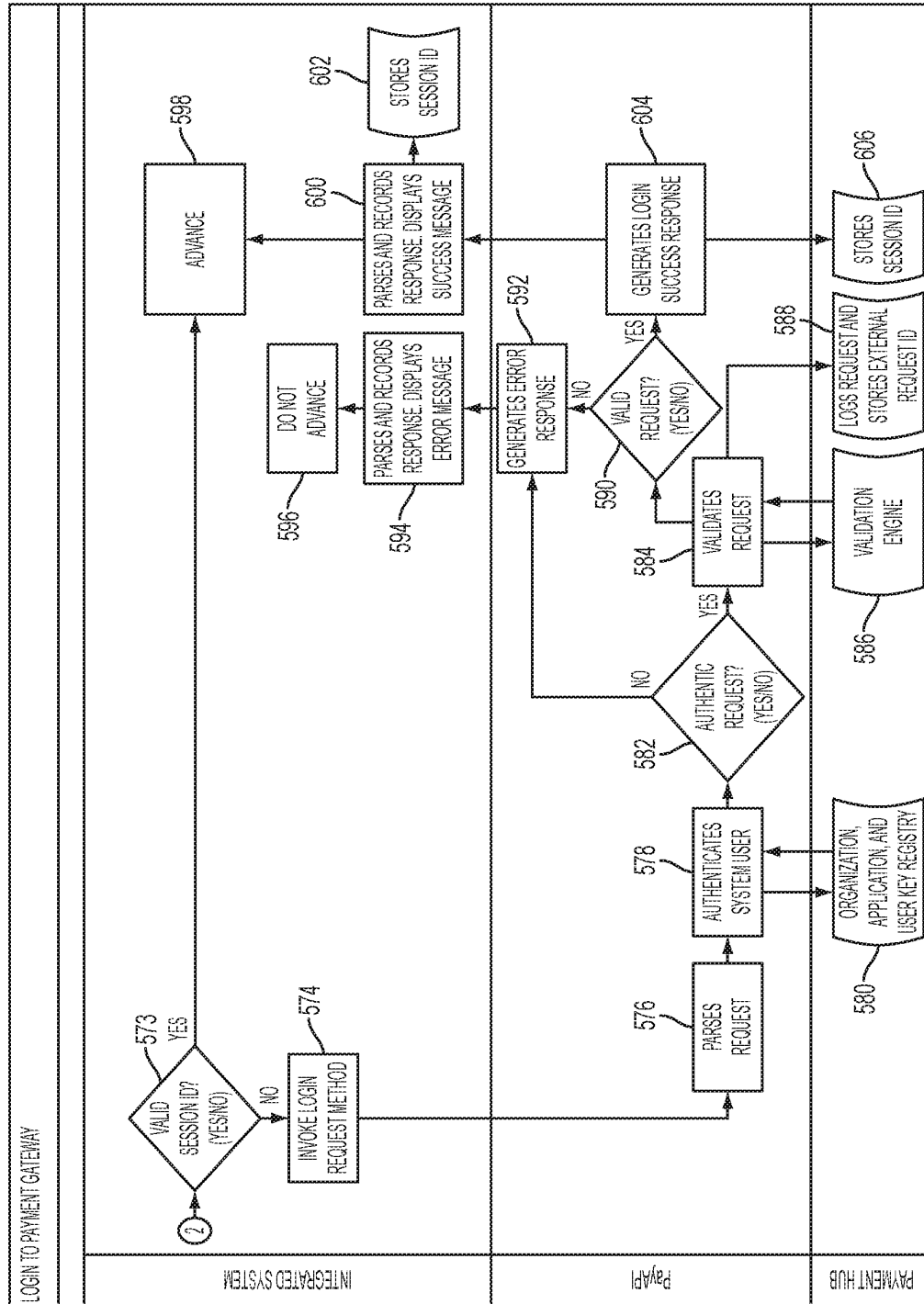


FIG. 4f

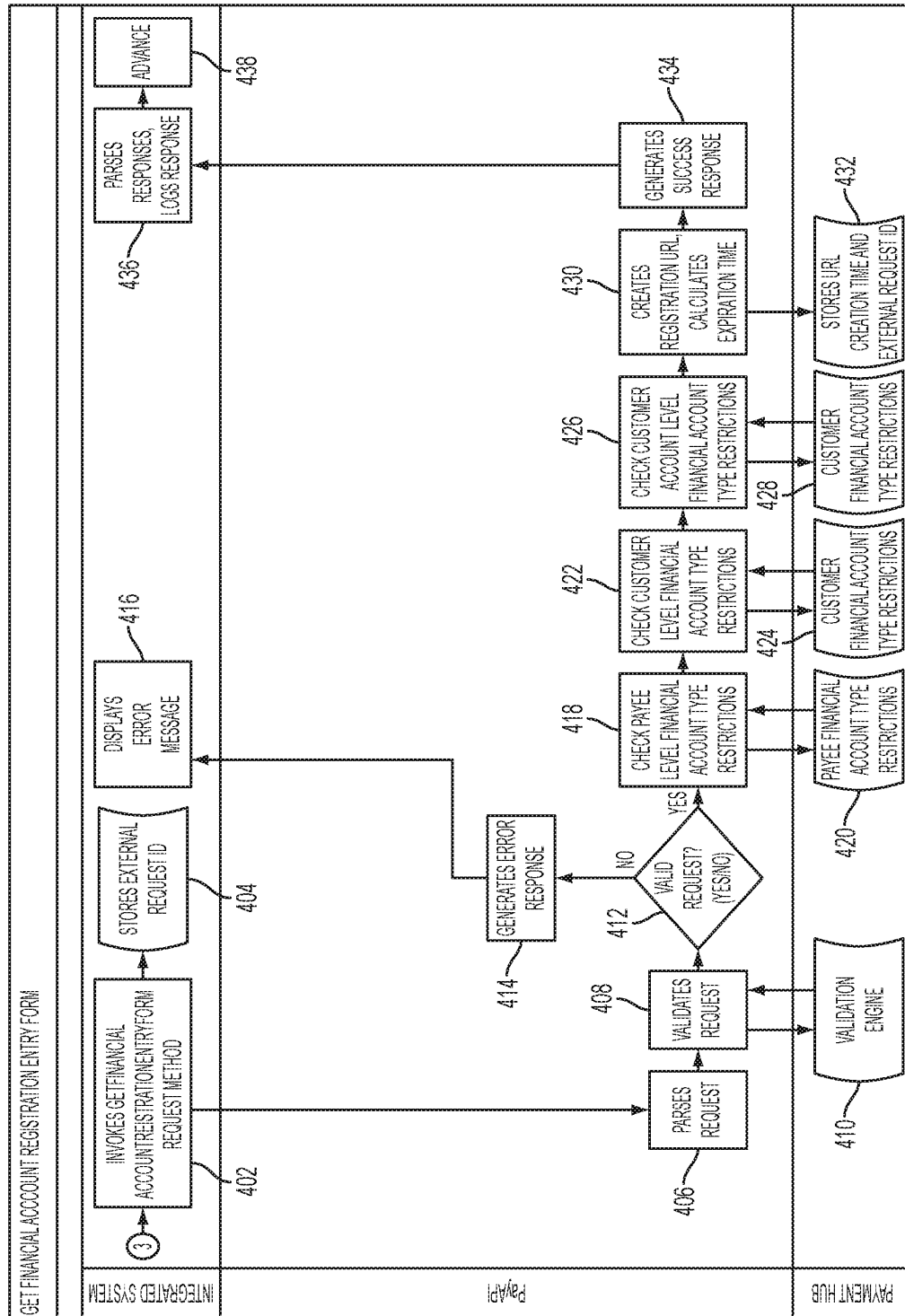


FIG. 4g

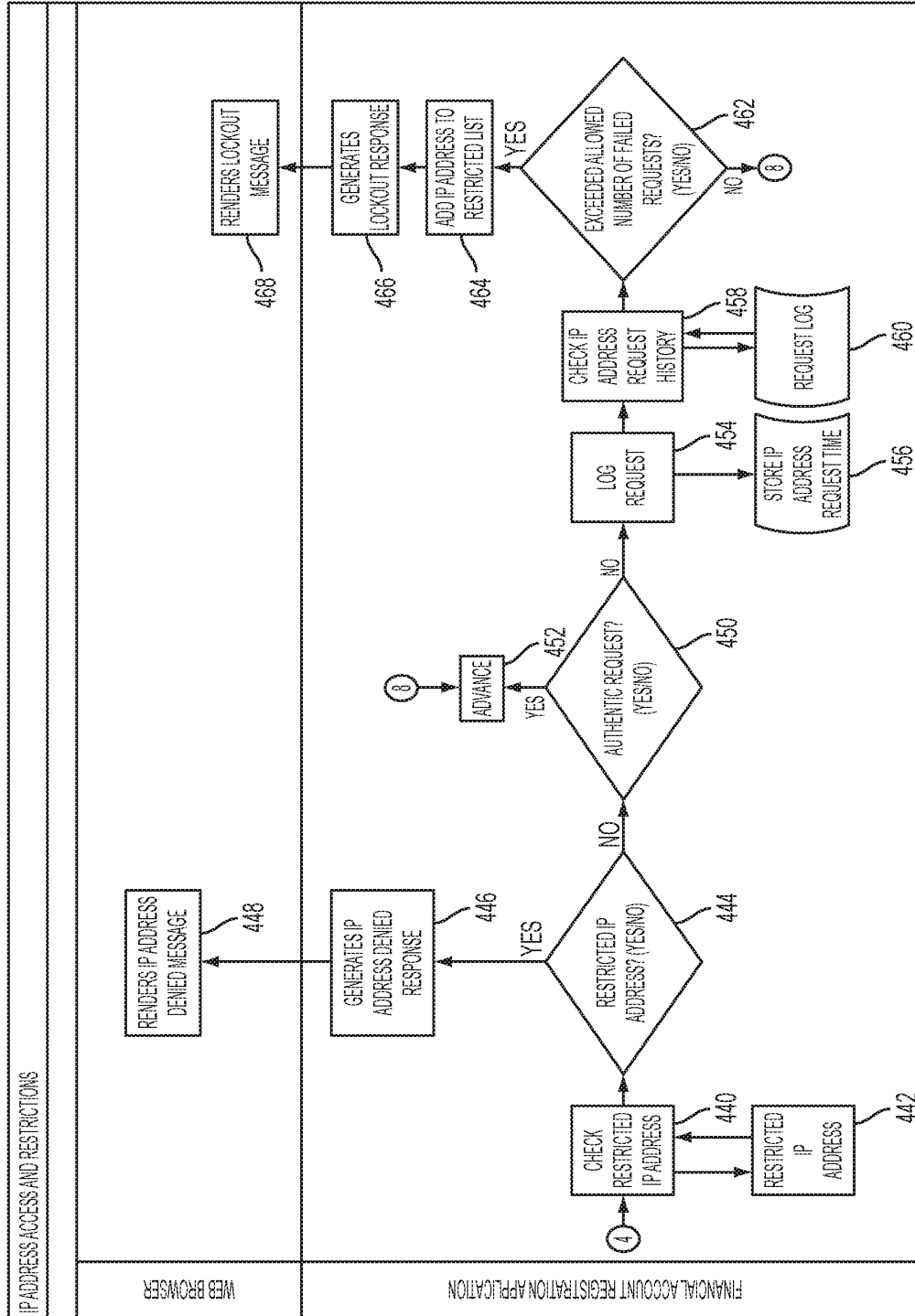


FIG. 4h

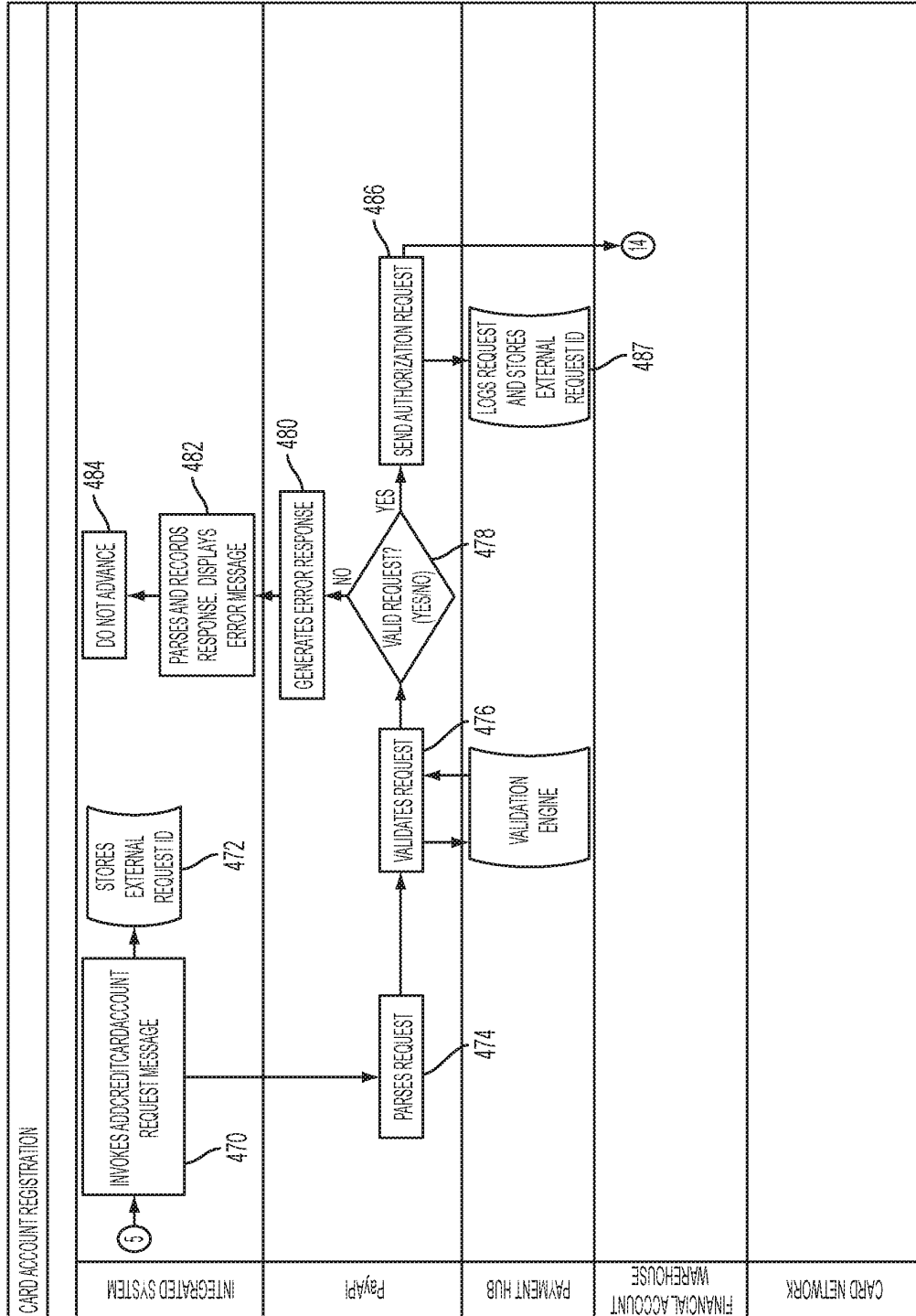


FIG. 4i

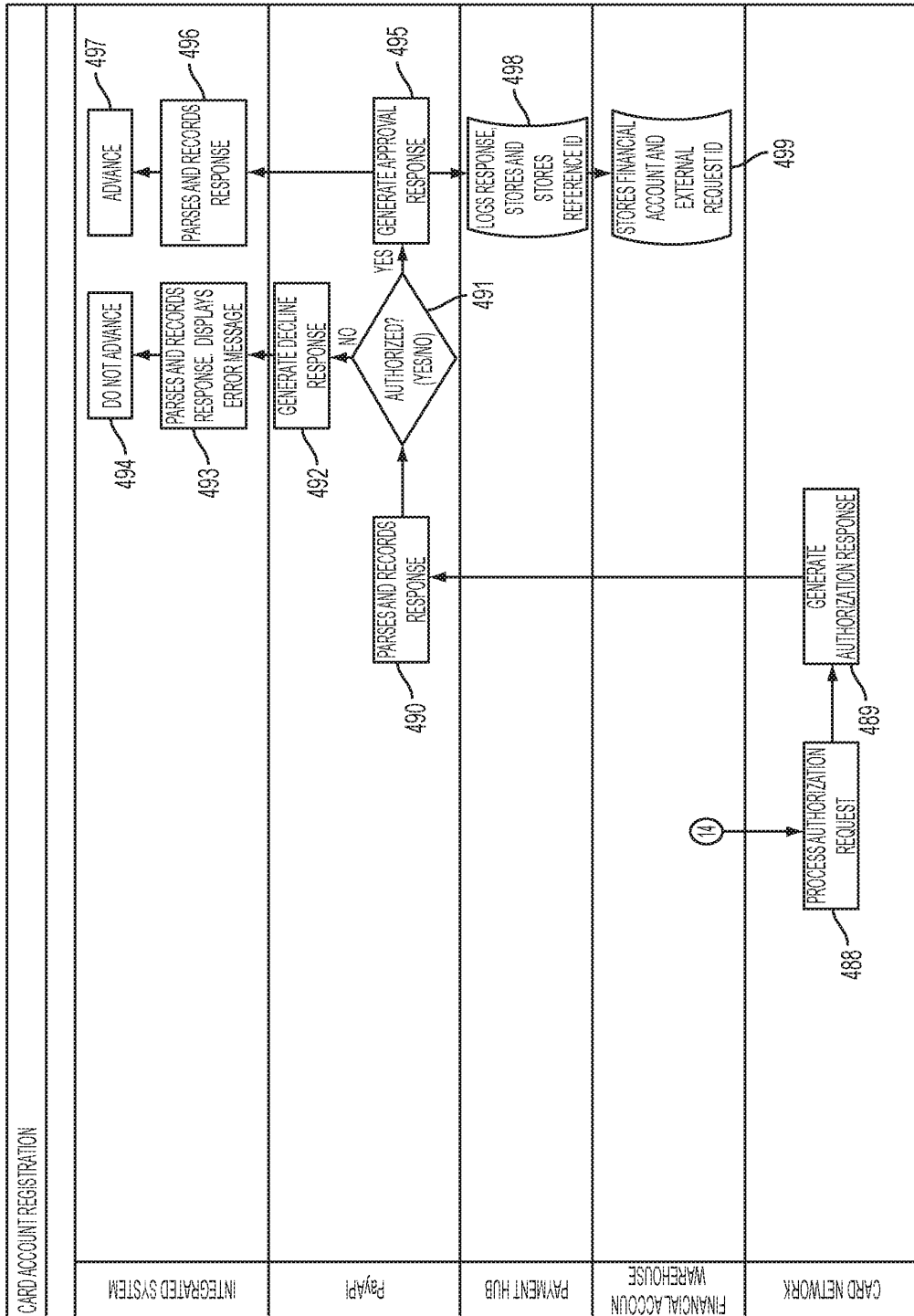


FIG. 4j

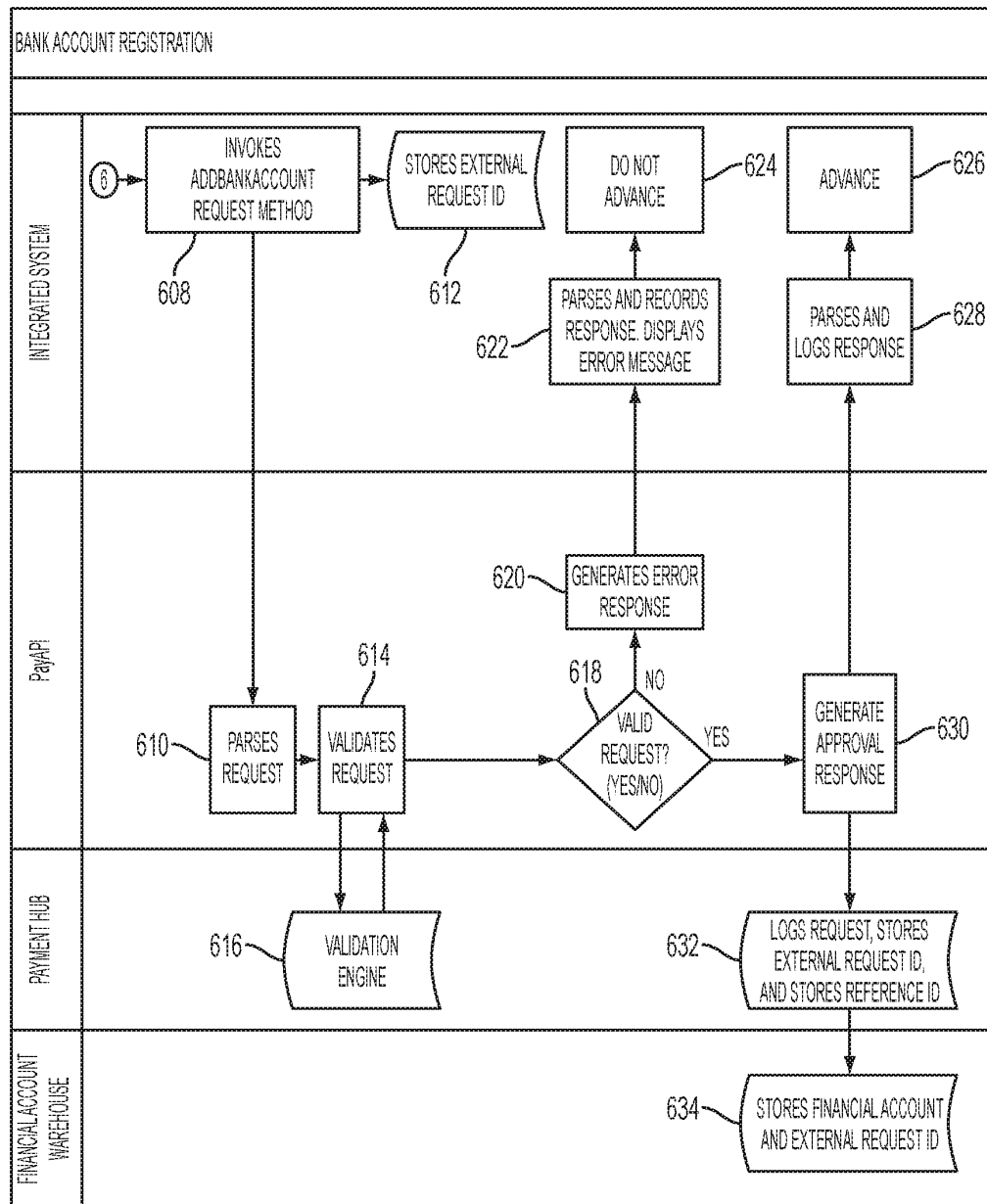


FIG. 4k

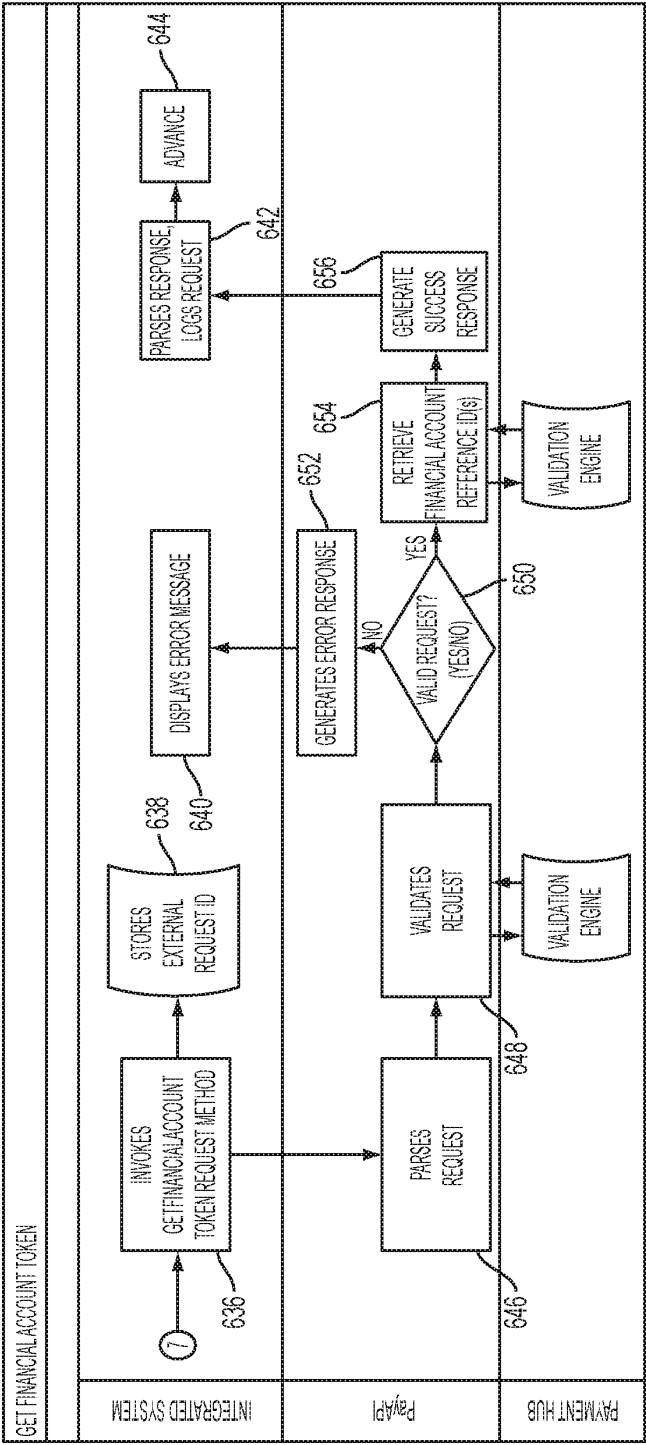


FIG. 4I

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: 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.

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.

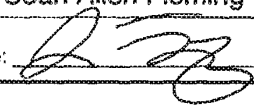
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

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: 

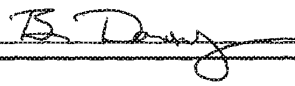
Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

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.

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: <u>Brian Edward Downey, Jr.</u> Date (Optional): <u>16 November 2012</u> Signature: <u></u> 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/D1 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.