

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PLAID INC.,
Petitioner,

v.

SIX TREES CAPITAL LLC,
Patent Owner According to PTO Assignment Records, and

SECURE AUTHENTICATION TECHNOLOGIES LLC,
Patent Owner Identified in Patent Complaint.

Case No. IPR2026-00157

U.S. Patent No. 11,315,090

Petition for *Inter Partes* Review of U.S. Patent No. 11,315,090

Mail Stop **PATENT BOARD**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

PETITIONER’S EXHIBIT LIST	v
TABLE OF ABBREVIATIONS	vi
MANDATORY NOTICES.....	vii
A. Real Parties-in-Interest [37 C.F.R. § 42.8(b)(1)]	vii
B. Related Matters [37 C.F.R. § 42.8(b)(2)].....	vii
C. Lead and Back-Up Counsel [37 C.F.R. § 42.8(b)(3)].....	vii
D. Service Information [37 C.F.R. § 42.8(b)(4)]	viii
I. INTRODUCTION	1
II. REQUIREMENTS OF <i>INTER PARTES</i> REVIEW	4
A. Standing.....	4
B. Identification of Challenge and Relief Requested	4
1. U.S. Patent Appl. Publ. No. 2008/0115198 (“Hsu”) (Ex-1004)	5
2. U.S. Patent No. US 8,261,334 (“Hazlehurst”) (Ex-1005)	6
3. U.S. Patent Appl. Publ. No. 2009/0198615 (“Emerson”) (Ex-1006)	6
4. Laerte Peotta <i>et al.</i> , <i>A Formal Classification of Internet Banking Attacks and Vulnerabilities</i> (“Peotta”) (Ex-1007).....	6
5. <i>Could My Bank’s Two-Factor Authentication be Hacked?</i> (“2FA Q&A”) (Ex-1009).....	7
C. How the Challenged Claims Are to be Construed Under 37 C.F.R. § 42.104(b)(3)	8
D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4).....	8
E. Supporting Evidence Under 37 C.F.R. §42.104(b)(5)	9

F.	Payment of Fees	9
III.	TECHNICAL BACKGROUND	9
A.	State of the Art	9
B.	Summary of the Prosecution History of the '090 patent.....	12
C.	Person of Ordinary Skill in the Art	13
IV.	GROUND OF UNPATENTABILITY.....	14
A.	Ground 1: Anticipation by Hsu (Claims 1, 4–6, and 9–10)	14
1.	Summary of Hsu (Ex-1004).....	14
2.	Detailed Analysis of Ground 1	17
a)	Claim 1.....	17
b)	Claim 4.....	28
c)	Claim 5.....	29
d)	Claim 6.....	29
e)	Claim 9.....	32
f)	Claim 10.....	32
B.	Ground 2: Anticipation by Hazlehurst (Claims 1, 4–6, and 9–10).....	32
1.	Summary of Hazlehurst (Ex-1005).....	32
2.	Detailed Analysis of Ground 2	34
a)	Claim 1.....	34
b)	Claim 4.....	46
c)	Claim 5.....	48
d)	Claim 6.....	48

e)	Claim 9.....	50
f)	Claim 10.....	50
C.	Ground 3: Obviousness Over Emerson in view of Hsu (Claims 1, 4–6, and 9–10).....	50
1.	Summary of Emerson (Ex-1006).....	50
2.	Motivation to Combine Emerson and Hsu	53
3.	Detailed Analysis of Ground 3	55
a)	Claim 1.....	55
b)	Claim 4.....	67
c)	Claim 5.....	68
d)	Claim 6.....	69
e)	Claim 9.....	73
f)	Claim 10.....	73
D.	Grounds 4, 5, and 6: Obviousness Over Hsu, Hazlehurst, or Emerson/Hsu in view of Peotta (Claims 2, 3, 7, and 8).....	73
1.	Summary of Peotta.....	73
2.	Motivation to Combine Hsu, Hazlehurst, or Emerson/Hsu with Peotta.....	75
3.	Detailed Analysis of Grounds 4, 5, and 6	78
a)	Claim 2.....	78
b)	Claim 3.....	82
c)	Claim 7.....	82
d)	Claim 8.....	83
E.	Grounds 7, 8, and 9: Obviousness Over Hsu, Hazlehurst, or Emerson/Hsu in view of 2FA Q&A (Claims 2, 3, 7, and 8).....	83

1.	Summary of 2FA Q&A.....	83
2.	Motivation to Combine Hsu, Hazlehurst, or Emerson/Hsu with 2FA Q&A.....	84
3.	Detailed Analysis of Grounds 7, 8, and 9	86
a)	Claim 2.....	86
b)	Claim 3.....	89
c)	Claim 7.....	90
d)	Claim 8.....	90
V.	ENABLEMENT AND SECONDARY CONSIDERATIONS	90
VI.	CONCLUSION.....	90
	APPENDIX: CHALLENGED CLAIM LISTING	95

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 11,315,090
1002	File History for U.S. Patent No. 11,315,090
1003	Declaration of Alex C. Snoeren, Ph.D.
1004	U.S. Patent Appl. Pub. No. 2008/0115198
1005	U.S. Patent No. 8,261,334
1006	U.S. Patent Appl. Pub. No. 2009/0198615
1007	Laerte Peotta <i>et al.</i> , <i>A Formal Classification of Internet Banking Attacks and Vulnerabilities</i> , 3 Int'l J. Comput. Sci. & Tech. 186 (Feb. 2011)
1008	<i>International Journal of Computer Science & Information Technology (IJCSIT)</i> , February 2011, Volume 3, Number 1, Academy & Industry Research Collaboration Center (AIRCC), https://web.archive.org/web/20110302081810/http://airccse.org/journal/ijcsit2011_curr.html (archived Mar. 2, 2011)
1009	<i>Could My Bank's Two-Factor Authentication be Hacked?</i> , IT Security Stack Exchange, https://web.archive.org/web/20130609185904/https://security.stackexchange.com/questions/36609/could-my-banks-two-factor-authentication-be-hacked (May 29, 2013) (archived June 9, 2013)
1010	Irv Englander, <i>The Architecture of Computer Hardware, System Software, and Network</i> , Chapters 1, 2, 7, and 8(4th ed. 2009)
1011	Declaration of Mary Bolin, Ph.D.
1012	Declaration of Mina Ching

TABLE OF ABBREVIATIONS

Abbreviation	Term
'090 patent	U.S. Patent No. 11,315,090 (Ex-1001)
AIA	America Invents Act
Challenged Claims	Claims 1–10 of U.S. Patent No. 11,315,090
Emerson	U.S. Patent Appl. Pub. No. 2009/0198615 (Ex-1006)
Ex-	Exhibit
Fig.	Figure
Hazlehurst	U.S. Patent No. 8,261,334 (Ex-1005)
Hsu	U.S. Patent Appl. Pub. No. 2008/0115198 (Ex-1004)
IPR	<i>inter partes</i> review
MFA	multi-factor authentication
Patent Owner	Six Trees Capital, LLC and/or Secure Authentication Technologies LLC
Peotta	Laerte Peotta <i>et al.</i> , <i>A Formal Classification of Internet Banking Attacks and Vulnerabilities</i> , 3 Int'l J. Comput. Sci. & Tech. 186 (Feb. 2011) (Ex-1007)
Petitioner	Plaid Inc.
POSITA	Person[s] of ordinary skill in the art
2FA Q&A	<i>Could My Bank's Two-Factor Authentication be Hacked</i> , IT Security Stack Exchange (May 29, 2013) (archived June 9, 2013) (Ex-1009)

MANDATORY NOTICES

A. Real Parties-in-Interest [37 C.F.R. § 42.8(b)(1)]

The real party-in-interest is Petitioner Plaid Inc. No other entity is funding, controlling, or directing this Petition, or otherwise has had an opportunity to control or direct this Petition or Petitioner's participation in any resulting *inter partes* review (IPR). According to the USPTO Assignment Records, the owner of the '090 patent is currently Six Trees Capital LLC. A complaint filed against Petitioner on June 26, 2025 alleges that Secure Authentication Technologies LLC is the patent owner of the '090 patent.

B. Related Matters [37 C.F.R. § 42.8(b)(2)]

The '090 patent that is the subject of this Petition is also the subject of a patent litigation suit brought by Secure Authentication Technologies LLC against Petitioner. *Secure Authentication Techs. LLC. v. Plaid Inc.*, C.A. No. 25-00514-DAK-JCB (JFM) (D. Utah filed June 26, 2025).

C. Lead and Back-Up Counsel [37 C.F.R. § 42.8(b)(3)]

Pursuant to 37 C.F.R. §§ 42.8(b)(3), 42.8(b)(4), and 42.10(a), Petitioner provides the following designation of counsel:

Lead Counsel for Petitioner	Back-up Counsel for Petitioner
Brian M. Buroker (Reg. No. 39,125) Gibson, Dunn & Crutcher LLP 1700 M Street, N.W. 7th Floor Washington, DC 20036-4504 Phone: (202) 955-8500 Fax: (202) 467-0539 Email: bburoker@gibsondunn.com	Brian Rosenthal <i>(pro hac vice forthcoming)</i> Gibson, Dunn & Crutcher LLP 200 Park Avenue New York, NY 10166 Phone: (212) 351-2339 Email: broenthal@gibsondunn.com <u>Additional Back-up Counsel</u> Jaysen S. Chung (Reg. No. 68,199) Gibson, Dunn & Crutcher LLP One Embarcadero Center, Suite 2600 San Francisco, CA 94111-3715 Phone: (415) 393-8271 Email: jschung@gibsondunn.com Hannah L. Bedard <i>(pro hac vice forthcoming)</i> Gibson, Dunn & Crutcher LLP 1700 M Street, N.W. 7th Floor Washington, DC 20036-4504 Phone: (202) 777-9579 Email: hbedard@gibsondunn.com

A Power of Attorney accompanies this Petition in accordance with 37 C.F.R. § 42.10(b).

D. Service Information [37 C.F.R. § 42.8(b)(4)]

Service via hand delivery or postal mail may be made at the address of the lead and back-up counsel above. Petitioner hereby consents to electronic service, and service by electronic mail may be made at the following email address:

GDCPlaidSAT@gibsondunn.com

I. INTRODUCTION

Pursuant to 35 U.S.C. § 311, Petitioner hereby petitions for *inter partes* review of U.S. Patent No. 11,315,090 (Ex-1001) and seeks cancellation of claims 1–10 as unpatentable under 35 U.S.C. §§ 102 and 103.

The Challenged Claims should not have been issued in their current form, as they fail to meet both the substantive requirements of patentability and the procedural integrity of the examination process.

Substantively, the Challenged Claims add nothing novel or inventive to the state of the art, as will be demonstrated through the evidence and expert declaration in this Petition. The Challenged Claims of the '090 patent are directed to a “method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol.” Ex-1001, claims 1, 6. The alleged invention of the '090 patent is described in the context of “optimizing the distribution of financial assets among financial accounts via a fully-automated approach that does not require user intervention on an ongoing basis.” *Id.*, 1:18–22. Specifically, the financial management system detailed in the '090 patent can “act as proxy for the user and respond to any multi-factor authentication that may be required for account access in a way that does not require user intervention.” *Id.*, 18:55–58.

The use of multi-factor authentication (MFA) to secure online accounts was well-known in the art prior to the '090 patent. Financial institutions have long required users to provide combinations of passwords, tokens, and biometric features to access their accounts. These security measures, however, have created obstacles for automated systems—like the financial management system in the '090 patent—seeking to access the accounts on behalf of users. In response, techniques to enable a third-party system to collect, encrypt, store, and retrieve user credentials, as well as process MFA requests—just like those described in the '090 patent—were developed well in advance of the effective filing date of the '090 patent.

The prior art references used in this Petition illustrate exactly that. For example, Hsu discloses a financial program that requests and receives encrypted MFA information (including user's credentials) from the user. Ex-1004, [0023]. Hazlehurst discloses a system that provides pre-stored user credentials and performs MFA on behalf of a user. Ex-1005, Abstract, 3:33–34. Emerson discloses an agent that provides MFA for online banking without user intervention. Ex-1006, [0053], [0060]. Specifically, claims 1, 4–6, and 9–10, which are directed to the very concept of permitting a third party to securely access online accounts protected by MFA, are anticipated by Hsu (**Ground 1**) and Hazlehurst (**Ground 2**), and are obvious in view of Emerson and Hsu (**Ground 3**).

The remaining dependent claims (*i.e.*, claims 2, 3, 7, and 8) are obvious over the prior art. These claims focus on allowing a third party to access an online account through a phone number or an email address, without an account holder's intervention. However, it was well-known in the prior art, including Peotta and 2FA Q&A, that authentication codes for an account can be sent to a phone number via SMS, and that a third party can gain access to the account by having those codes sent to a number they control. Ex-1007, 5; Ex-1009, 1. As will be shown in this Petition, claims 2, 3, 7, and 8 are obvious in view of Hsu and Peotta (**Ground 4**); Hazlehurst and Peotta (**Ground 5**); Emerson, Hsu, and Peotta (**Ground 6**); Hsu and 2FA Q&A (**Ground 7**); Hazlehurst and 2FA Q&A (**Ground 8**); and Emerson, Hsu, and 2FA Q&A (**Ground 9**).

Given the prior art, these claims should never have issued. In addition, the prosecution history demonstrates that the Patent Office likely made a mistake in issuing these claims in their present form. Specifically, prior to allowance, dependent claims 2 and 7 were canceled and the independent claims were amended via an examiner's amendment, authorized by the applicants, to include "endpoint" elements originally recited in the cancelled dependent claims. Ex-1002, 498–500 ("Authorization for this examiner's amendment was given in an email from Applicants' representative on 2-4-2022."). But without any explanation, the Patent Office issued the claims without including the examiner's amendment and without

canceling dependent claims 2 and 7, in what appears to be an error. *Id.*, 543; Ex-1001, claims 1–10.

In view of the foregoing, Petitioner respectfully requests the cancellation of the Challenged Claims.

II. REQUIREMENTS OF *INTER PARTES* REVIEW

A. Standing

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '090 patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR on the grounds identified herein.

B. Identification of Challenge and Relief Requested

Pursuant to 37 C.F.R. § 42.104(b), Petitioner requests that the Board institute IPR of claims 1–10 of the '090 patent under 35 U.S.C. §§ 102 and 103.

The '090 patent issued from an application filed April 16, 2020, and claims priority to an application filed January 28, 2014. For purposes of this Petition only, Petitioner does not dispute that the Challenged Claims are entitled to an effective filing date of January 28, 2014.

The precise relief requested by Petitioner is that claims 1–10 be canceled based on the grounds below:

Ground	Claims	Basis for Rejection¹
1	1, 4–6, and 9–10	Anticipation by Hsu
2	1, 4–6, and 9–10	Anticipation by Hazlehurst
3	1, 4–6, and 9–10	Obviousness over Emerson in view of Hsu
4	2, 3, 7, 8	Obviousness over Hsu in view of Peotta
5	2, 3, 7, 8	Obviousness over Hazlehurst in view of Peotta
6	2, 3, 7, 8	Obviousness over Emerson/Hsu in view of Peotta
7	2, 3, 7, 8	Obviousness over Hsu in view of 2FA Q&A
8	2, 3, 7, 8	Obviousness over Hazlehurst in view of 2FA Q&A
9	2, 3, 7, 8	Obviousness over Emerson/Hsu in view of 2FA Q&A

The above challenges are made in view of the following prior art references:

1. U.S. Patent Appl. Publ. No. 2008/0115198 (“Hsu”) (Ex-1004)

U.S. Patent Appl. Publ. No. 2008/0115198 (“Hsu”), titled “Multi-Factor Authentication Transfer,” published on May 15, 2008, from an application filed on October 31, 2006. Ex-1004. Hsu qualifies as prior art to the ’090 patent under at least AIA 35 U.S.C. § 102(a)(1). Hsu was not considered during prosecution of the ’090 patent.

¹ All obviousness grounds include the knowledge of POSITA.

2. U.S. Patent No. US 8,261,334 (“Hazlehurst”) (Ex-1005)

U.S. Patent No. US 8,261,334 (“Hazlehurst”), titled “System for Performing Web Authentication of a User by Proxy,” issued on September 4, 2012, from an application filed on April 25, 2008. Ex-1005. Hazlehurst qualifies as prior art to the ’090 patent under at least AIA 35 U.S.C. § 102(a)(1). Hazlehurst was not considered during prosecution of the ’090 patent.

3. U.S. Patent Appl. Publ. No. 2009/0198615 (“Emerson”) (Ex-1006)

U.S. Patent Appl. Publ. No. 2009/0198615 (“Emerson”), titled “Method, Device, and System for Completing On-Line Financial Transaction,” published on August 6, 2009, from an application filed on February 1, 2008. Ex-1006. Emerson qualifies as prior art to the ’090 patent under at least AIA 35 U.S.C. § 102(a)(1). Emerson was not considered during prosecution of the ’090 patent.

4. Laerte Peotta *et al.*, *A Formal Classification of Internet Banking Attacks and Vulnerabilities* (“Peotta”) (Ex-1007)

A Formal Classification of Internet Banking Attacks and Vulnerabilities, by Laerte Peotta *et al.*, was published in the February 2011 issue of the International Journal of Computer Science & Information Technology (IJCSIT). Ex-1007, 1; Ex-1011, ¶¶21–26, 29. Peotta qualifies as prior art to the ’090 patent under at least AIA 35 U.S.C. § 102(a)(1). Peotta was not considered during prosecution of the ’090 patent.

Peotta was publicly available to interested persons to download directly from the IJCSIT website by at least March 2, 2011. Ex-1008, 2; Ex-1011, ¶¶27–30. The IJCSIT website was indexed by numerous search engines including Google Scholar and WorldCat by at least September 17, 2011. Ex-1011, ¶31. A POSITA looking to employ a method to automate authentication and authorization for Internet banking applications would have easily located Peotta by typing related keywords into these search engines. Ex-1003, ¶171; Ex-1011, ¶¶32–36. For example, Peotta was one of the front-page results provided by Google Scholar when searching for “Internet banking authentication authorization” before the effective filing date of the ’090 patent. Ex-1003, ¶170.

**5. *Could My Bank’s Two-Factor Authentication be Hacked?*
 (“2FA Q&A”) (Ex-1009)**

Could My Bank’s Two-Factor Authentication be Hacked? (“2FA Q&A”) is a question posted (and answered) on IT Security Stack Exchange on May 29, 2013. Ex-1009, 1. 2FA Q&A qualifies as prior art to the ’090 patent under 35 U.S.C. § 102(a)(1). 2FA Q&A was not considered during prosecution of the ’090 patent.

2FA Q&A was publicly available to interested persons to access via the Internet by at least June 9, 2013. Ex-1012, ¶¶4, 6. Stack Exchange, where 2FA Q&A was published, was indexed by popular search engines like Google prior to the effective filing date of the ’090 patent. Ex-1003, ¶188. A POSITA would have

turned to search engines like Google to locate existing methods using relevant keywords. Ex-1003, ¶¶189–90. 2FA Q&A was one of the front-page results returned by Google when searching for “multi-factor authentication phone number internet banking” before the effective filing date of the ’090 patent. *Id.*

C. How the Challenged Claims Are to be Construed Under 37 C.F.R. § 42.104(b)(3)

A claim subject to IPR shall be construed using the same standard as in a civil action. 37 C.F.R. § 42.100(b). The Board need only construe terms “to the extent necessary to resolve the controversy.” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioner submits that no construction of any claims term is necessary for the Board to resolve this Petition. Petitioner maintains that the Challenged Claims would have been anticipated and/or obvious under any reasonable construction. As discussed in the detailed grounds below, the claims are unpatentable regardless of whether the preamble is limiting.

D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4)

An explanation of how the Challenged Claims are unpatentable under the statutory grounds identified above, including the identification of where each element of the claim is found in the prior art patents or printed publications, is provided below.

E. Supporting Evidence Under 37 C.F.R. §42.104(b)(5)

The exhibit numbers of the supporting evidence relied upon and the relevance of the evidence to the Challenged Claims, including an identification of specific portions of the evidence that support the challenge, are provided below. A list of exhibits is also included in this petition pursuant to 37 C.F.R. § 42.63(e). The technical information and grounds for rejection explained in the Petition are further supported by the Declaration of Alex C. Snoeren, Ph.D. (Ex-1003).

F. Payment of Fees

Pursuant to 37 C.F.R. §§ 42.103 and 42.15(a), the required fee is being submitted herewith. The Office is authorized to charge any fee deficiency, or credit overpayment, to Deposit Account 50-1408, including additional fees due in connection with this Petition.

III. TECHNICAL BACKGROUND

A. State of the Art

MFA was a standard security measure for protecting online accounts, especially in the financial sector, before the '090 patent. Ex-1003, ¶¶47–48. MFA typically requires users to provide multiple forms of credentials, such as passwords, tokens, or biometric data, to verify their identity. Ex-1004, [0003]; Ex-1005, 1:53–2:20, 2:30–38; Ex-1006, [0059]. Because MFA process is designed to require direct user intervention, it creates significant obstacles for automated systems that

need access to these accounts on behalf of users. Ex-1003, ¶49; Ex-1004, [0004]–[0005]; Ex-1005, 2:21–29.

Three prior art references in this Petition—Hsu, Hazlehurst, and Emerson—address this challenge by disclosing methods that enable third-party systems to securely access MFA-protected accounts without ongoing user involvement. Ex-1003, ¶¶49–51. Hsu discloses a financial program that requests and receives MFA information from the user. Ex-1004, [0023]. The program then encrypts and stores the collected user credentials, which are used to access the user’s account in the future. *Id.*, [0031], [0035], [0039]. Hazlehurst describes a system where a portal server (PS) and a Pin Vault Application (PVA) work together to perform authentication on behalf of the user. Ex-1005, Abstract. User credentials are prestored in an encrypted pin vault for PS/PVA to access when handling MFA requests such as tokens and CAPTCHA. *Id.*, 4:48–67, 8:14–27, 9:7–20. Emerson presents a method for conducting secure online transactions using an ODS agent that interacts with financial institutions. Ex-1006, [0053]. The ODS agent collects authentication credentials and caches device tokens for future use, enabling the automation of the authentication process. *Id.*, [0060], [0069]. The figure below is representative of their shared multi-party architecture (*e.g.*, **user**, **bank**, and **third party**):

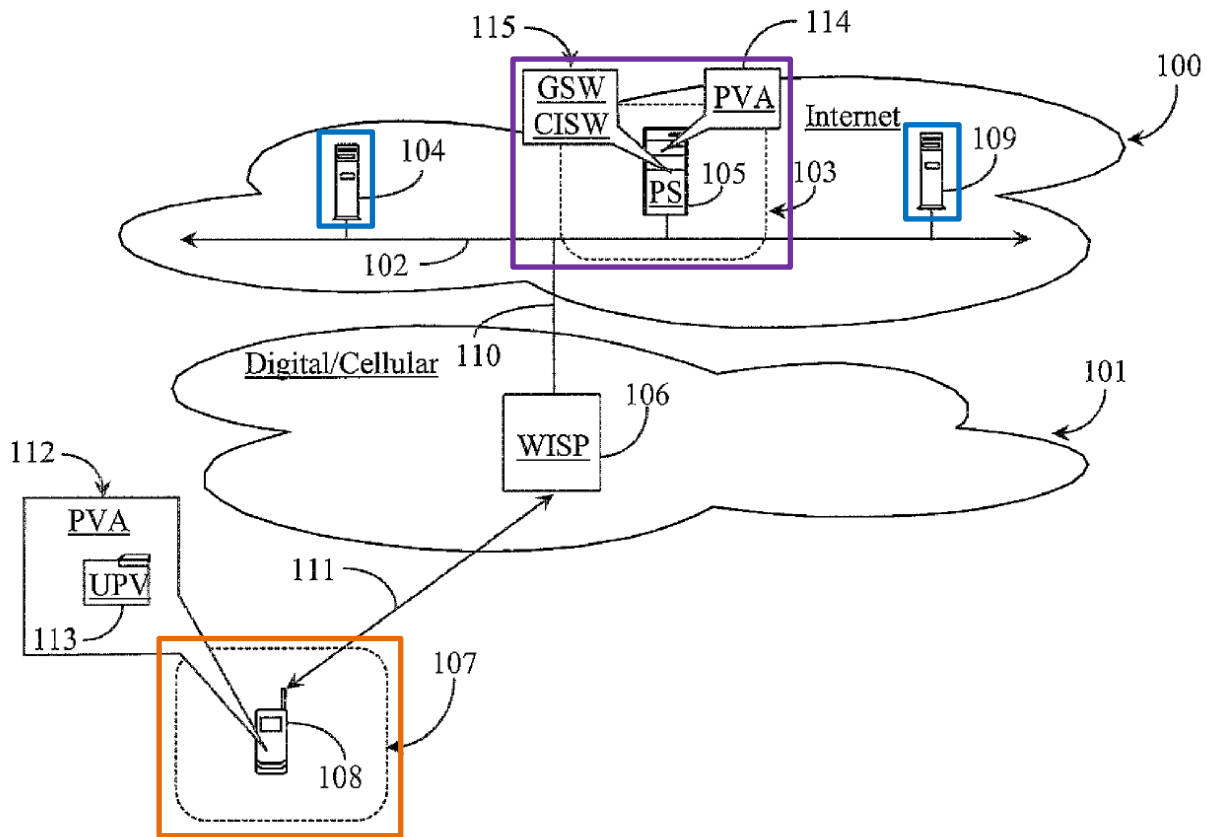


Fig. 1

Ex-1005, Fig. 1 (annotated).

Beyond the core architecture, Peotta and 2FA Q&A introduce the concept of using endpoints, such as phone numbers, to facilitate automated responses to MFA challenges. Ex-1003, ¶¶52–53. Peotta analyzes vulnerabilities in SMS-based authentication for online banking, noting that attackers (*i.e.*, third parties) can alter the phone number to which authentication messages are sent. Ex-1007, 5. This technique allows a third party to receive MFA codes directly and enables automated access without user intervention. *Id.* 2FA Q&A discusses how social engineering

can change the registered mobile phone number for an account and redirect MFA codes to a device controlled by a third party. Ex-1009, 1. This approach, while described as a vulnerability, is equally applicable to legitimate authentication scenarios, where a system updates the endpoint to facilitate automated access to an online account. Ex-1003, ¶¶180, 198.

B. Summary of the Prosecution History of the '090 patent

The '090 patent was filed on April 16, 2020 as Application No. 16/850,150 and claims priority to Provisional Application No. 61/932,495, filed on January 28, 2014. Ex-1001, 1.

The examiner initially rejected claims 1–3 as unpatentable as anticipated by Counterman (U.S. Patent No. 8,495,720), among other reasons. Ex-1002, 329–30. In response, the applicants amended the claims to require two additional steps—“collecting the account holder’s credentials” and “storing the account holder’s credentials using one or more processors, wherein the credentials are stored in a data store.” *Id.*, 370. After a 101 rejection, *id.*, 408–18, the applicants amended claims 1 and 6 to require yet another step—“encrypting the account holder’s credentials using one or more processors.” *Id.*, 457–59.

In the Notice of Allowance dated March 11, 2022, the examiner cancelled claims 2 and 7, and amended claims 1, 3–6, and 8–10 by adding the “endpoint”

elements originally recited in claims 2 and 7 to claims 1 and 6, pursuant to the applicants' authorization in a February 4, 2022 e-mail. *Id.*, 498–501. Based on these amendments, the examiner concluded that the amended claims were patent-eligible and that Counterman did not teach each element of the amended claims. *Id.*, 501–03. Two weeks later, however, the examiner issued a Corrected Notice of Allowance that reverted claims 1–10 back to the version presented prior to the examiner's amendment, without any explanation, seemingly in error. *Id.*, 543. The '090 patent subsequently issued on April 26, 2022. Ex-1001, 1.

C. Person of Ordinary Skill in the Art

A POSITA would have had an undergraduate degree in computer science, electrical engineering, computer engineering, or similar technical field; and one to two years of experience in the analysis, design, development, and/or implementation of authentication protocols for Web applications, with additional education substituting for less experience and vice versa. Ex-1003, ¶25.

IV. GROUNDS OF UNPATENTABILITY

A. Ground 1: Anticipation by Hsu (Claims 1, 4–6, and 9–10)

1. Summary of Hsu (Ex-1004)

Hsu is directed to “techniques for collecting and providing authentication information.” Ex-1004, [0001]. Hsu explains that authentication is a “widely used procedure[]” that “enable[s] a user to access an application or system (by confirming the user’s identity) and to verify the authority of the user to perform certain operations or tasks.” Ex-1004, [0002]. As an example, Hsu discloses that a user may provide information, such as a username and a password, to confirm the user’s identity. *Id.* Hsu further explains that “[a]s security threats continue to grow, many applications and systems are significantly increasing such protection requirements,” and as a result, many applications and systems utilize multiple authentication factors to perform authentication (also referred to as multi-factor authentication).” *Id.*, [0003]. Such MFA may include “something the user knows (for example, a password), something the user has (for example, a token), and/or something the user is (for example, a biometric feature).” *Id.*

Hsu describes a “computer system 100” that includes computers and servers that are networked together, where one or more users may provide MFA information to a program, such as a financial program, that executes on computer 110. Ex-1004, [0027].

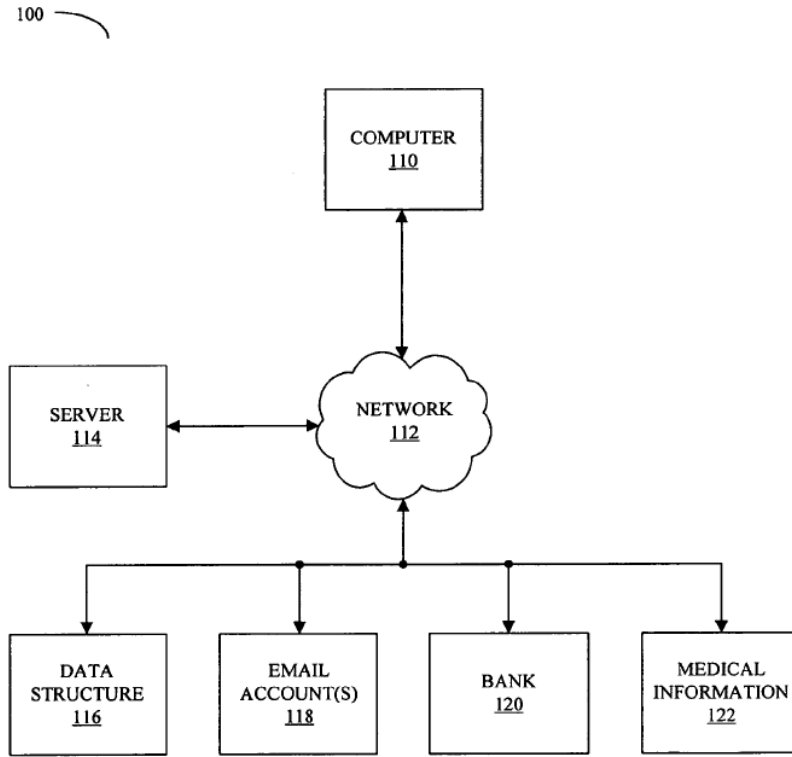


FIG. 1

Id., Fig. 1.

In addition, Hsu discloses a “computer system 200” that includes one or more processors 210, a communication interface 212, a user interface 214, and one or more signal lines 222 coupling these components together. *Id.*, [0040].

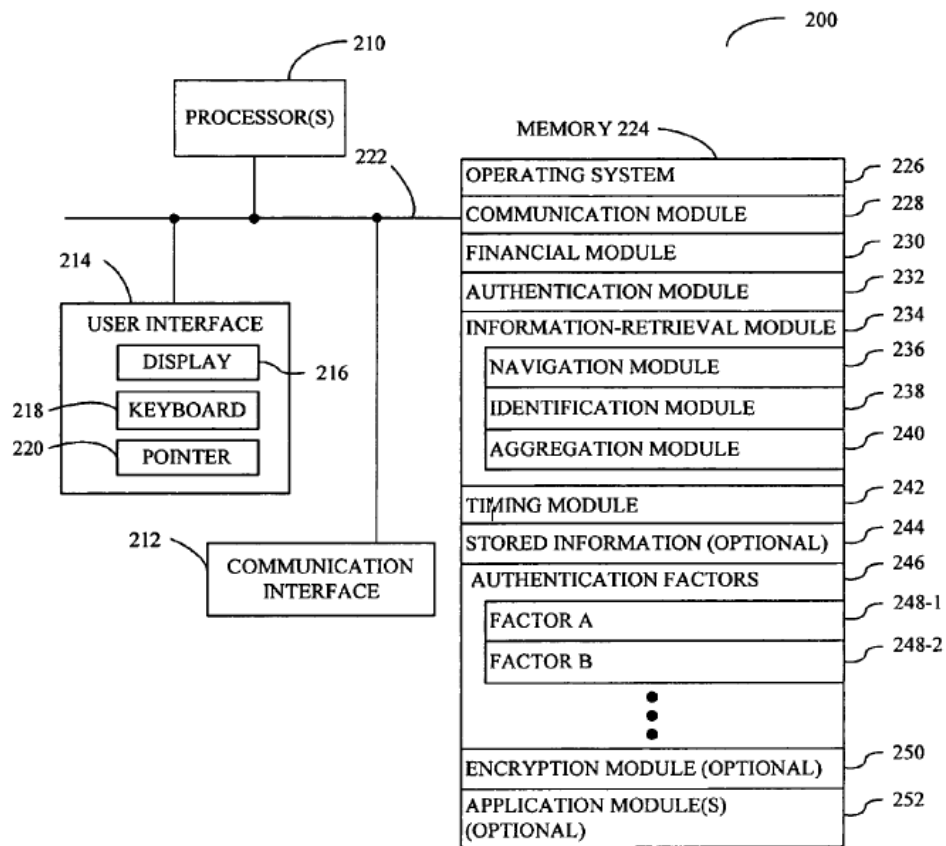


FIG. 2

Id., Fig. 2.

2. Detailed Analysis of Ground 1

a) Claim 1

(1) [1pre]

A method for permitting a **third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol**, comprising the following steps performed by the third-party entity,

Hsu discloses this element. Ex-1003, ¶¶59–64. For instance, Hsu discloses a “**computer system**” that “may be **used to retrieve information, such as financial information for a user** (for example, banking information), information associated with multiple email accounts for the user, and/or medical information for the user.”² Ex-1004, [0023]. The computer system in Hsu is usable by a third-party entity, such as a financial program or a financial application. *Id.*, [0031] (“the **financial program** may **access one or more documents (such as one or more websites or web pages on one or more hosts) and may retrieve stored information (such as financial information) for the user.**”); [0023] (“the application may include a **financial application**, such as Quicken™, TurboTax™, or other software capable of **receiving financial-related data, bank statements, and/or investment records**”).

² All emphasis added unless otherwise noted.

The user in Hsu is an account holder. As the following commands show, the financial program (*i.e.*, Customer Central or CC) requests the user to answer a question (*i.e.*, “In what city were you born?”) for the financial program to “[d]iscover” the user’s “[a]ccount[]” (*i.e.*, “CCDiscoverAccountsInteractiveResponse”) from the bank 120. *Id.*, [0035].

```
<?xml version="1.0" encoding="UTF-8"?>
<cc:CCWSResponse xmlns:cc="http://www.intuit.com/CustomerCentral">
  <status>
    <code>ok</code>
    <string>call successful</string>
  </status>
  <body>
    <ccresp:CCDiscoverAccountsInteractiveResponse
      xmlns:ccresp="http://www.intuit.com/CustomerCentral/Responses">
      <session>
        <cccaptureIpAddress>172.23.29.76</cccaptureIpAddress>
        <cccapturePort>9909</cccapturePort>
        <ccscrapeIpAddress>172.23.29.76</ccscrapeIpAddress>
        <ccscrapePort>9979</ccscrapePort>
        <ccscriptInstanceId>-208666287</ccscriptInstanceId>
      </session>
      <questions>
        <question>
          <text>In what city were you born? (Enter full name of city only)</text>
        </question>
      </questions>
    </ccresp:CCDiscoverAccountsInteractiveResponse>
  </body>
</cc:CCWSResponse>.
```

Id. (annotated).

The “stored authentication information and/or stored retrieved information are **encrypted**” and “may be **encrypted** when it is communicated over the network 112.” *Id.*, [0039]. Hsu’s method of gaining access is thus done in a secure manner. Ex-1003, ¶63.

The online account is secured by a MFA protocol, and therefore the user must “provide **multi-factor authentication** information to a program, such as a financial program,” so that the financial program can “assemble (i.e., retrieve) information for the user.” *Id.*, [0027], [0038]. That is, Hsu discloses “[u]sing the **multi-factor authentication**, [to enable] the **financial program** [to] **access one or more documents (such as one or more websites or web pages on one or more hosts) and may retrieve stored information (such as financial information) for the user.**” *Id.*, [0031].

(2) [1a]

collecting the account holder’s credentials;

Hsu discloses this element. Ex-1003, ¶¶65–67. Hsu discloses that the system “may request and receive” user credentials that are part of the MFA information Hsu receives and collects. Ex-1004, [0023]; [0027] (“One or more users may provide multi-factor authentication information to a program, such as a financial program, that executes on computer 110.”). The MFA information received includes user’s credentials, such as “one or more usernames, one or more passwords, one or more

pins, one or more telephone numbers, one or more addresses, and/or additional personal information.” *Id.*, [0029]; [0002] (“Authentication ... enable[s] a user to access an application or system (by confirming the user’s identity)”). The user in Hsu is an account holder. *Id.*, [0035] (“CCDiscoverAccountsInteractiveResponse”).

(3) [1b]

encrypting the account holder’s credentials using one or more processors;

Hsu discloses this element. Ex-1003, ¶68. For instance, Hsu explains that the MFA information, which includes account holder/user’s credentials, “may be a sensitive nature” and as a result, the “stored authentication information” is “encrypted.” Ex-1004, [0039]. Further, Hsu discloses an “**encryption module (or a set of instruction) 250**” executed on “**one or more processing units 210**” and thus, the encrypting occurs using one or more processors as claimed. *Id.*, [0040], [0043]–[0044].

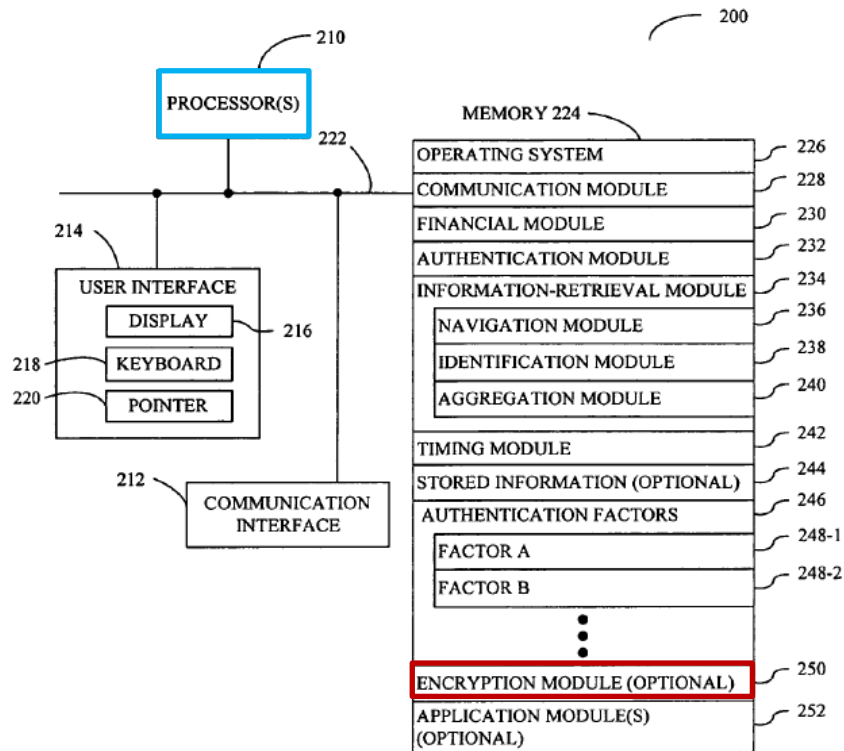


FIG. 2

Id., Fig. 2 (annotated).

(4) [1c]

storing the account holder’s encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;

Hsu discloses this element. Ex-1003, ¶¶69–71. Specifically, Hsu discloses that the system “stores the information and/or the multiple authentication factors on the first host.” Ex-1004, [0008]. In addition, Hsu discloses that the MFA information “may be initially *stored* locally on the computer 110 or remotely, for example, on the server 114, *in a data structure 116*,” which is a data store. *Id.*, [0031], [0026]. As shown in Figure 5, “this data structure 500 may include

authentication information for one or more users 510 of the financial program,” such as “user name,” “password,” and “personal information.” *Id.*, [0051]. Further, the “stored authentication information ... are *encrypted*.” *Id.*, [0039].

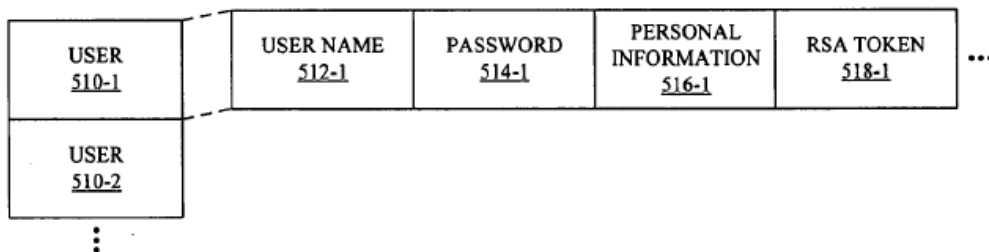


FIG. 5

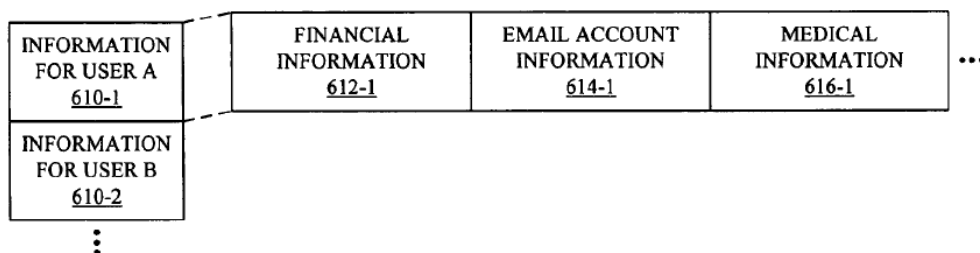


FIG. 6

Id., Figs. 5, 6.

The storage process is performed using “*one or more processors 210*” on the computer. *Id.*, [0040] (“The computer system 200 includes one or more processors 210”); [0041] (“Memory 224 may store an operating system 226 that includes procedures (or a set of instructions) for handling various basic system services for

performing hardware dependent tasks.”); [0044] (“Instructions in the various modules in the memory 224 may be implemented in a ... programming language The programming language may be ... executed by the one or more processing units 210.”).

(5) [1d]

verifying the account holder’s credentials by accessing, via one or more processors, the online account using the account holder’s credentials;

Hsu discloses this element. Ex-1003, ¶¶71–73. Hsu discloses a system that uses “multiple authentication factors from a user” (*i.e.*, using the account holder’s credentials) on a first host to “access [a] document” on a second host. Ex-1004, [0006]. Using authentication factors to access a document on a remote host requires accessing the user’s account with which both the authentication factors and the document are associated. *Id.*; Ex-1003, ¶71. For example, the system may request the user to answer a challenge question in order to “[d]iscover” the user’s “[a]ccount[]” and then to “request[] information from the bank 120.” Ex-1004, [0035]. As explained above, the user in Hsu is an account holder. *Id.*, [0035] (“CCDiscoverAccountsInteractiveResponse”).

Hsu further discloses that the account holder/user provides MFA information, such as usernames and passwords, to “enable [the] user to access an application or system (by confirming the user’s identity) and to verify the authority of the user to

perform certain operations or tasks.” *Id.*, [0002], [0027]–[0029]. “Using the multi-factor authentication information, the financial program may access one or more documents (such as one or more websites or web pages on one or more hosts) and may retrieve stored information (such as financial information) for the user.” *Id.*, [0031]. Therefore, the account holder/user’s documents could only be accessed after the account holder/user’s credentials were verified. Ex-1003, ¶72.

The online account is accessed via “one or more processors 210.” Ex-1004, [0040] (“The computer system 200 includes one or more processors 210”); [0041] (“The memory 224 may also store procedures (or a set of instructions) in a communication module 228. The communication procedures may be used for communicating with one or more computers and/or servers, including computers and/or servers that are remotely located with respect to the computer system 200.”); [0044] (“Instructions in the various modules in the memory 224 may be implemented in a ... programming language The programming language may be ... executed by the one or more processing units 210.”).

(6) [1e]

receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;

Hsu discloses this element. Ex-1003, ¶¶74–75. Hsu discloses that after the financial program requests access to the online account, the online account requires MFA information for access. Ex-1004, [0024] (“The application may utilize such multi-factor information to access a document (such as a website or web page) that is resident on a server computer.”). As shown below, “CCDiscoverAccounts” means that the financial program (*i.e.*, Customer Central or CC) requests the user to answer a question (city of birth) in order to “[d]iscover” (*i.e.*, access) the user’s “account[]” from the bank. *Id.*, [0035]; Ex-1003, ¶74. Hsu provides the following commands to demonstrate this request:

```

<?xml version="1.0" encoding="UTF-8"?>
<cc:CCWSResponse xmlns:cc="http://www.intuit.com/CustomerCentral">
  <status>
    <code>ok</code>
    <string>call successful</string>
  </status>
  <body>
    <ccresp:CCDiscoverAccountsInteractiveResponse
      xmlns:ccresp="http://www.intuit.com/CustomerCentral/Responses">
      <session>
        <cccaptureIpAddress>172.23.29.76</cccaptureIpAddress>
        <cccapturePort>9909</cccapturePort>
        <ccsrapeIpAddress>172.23.29.76</ccsrapeIpAddress>
        <ccsrapePort>9979</ccsrapePort>
        <ccscriptInstanceId>-208666287</ccscriptInstanceId>
      </session>
      <questions>
        <question>
          <text>In what city were you born? (Enter full name of city only)</text>
        </question>
      </questions>
    </ccresp:CCDiscoverAccountsInteractiveResponse>
  </body>
</cc:CCWSResponse>.

```

Id., [0035] (annotated). The bank (e.g., the host of the account holder’s online account) requires a response from the user to confirm which city the user was born, which Hsu explains is a type of “multi-factor authentication” (e.g., “something the user knows”). *Id.*, [0003], [0035], [0036].

(7) [1f]

prompting the account holder for a response and receiving the response thereto from the account holder; and

Hsu discloses this element. Ex-1003, ¶76. Hsu discloses that the answer to the requested authentication information (*i.e.*, “In what city were you born?”) may be prompted/requested from the account holder/user with the response being provided thereto. Ex-1004, [0035] (“The financial program may ... request the authentication information (city of birth) from the user”).

(8) [1g]

transmitting the account holder’s response to the online account to satisfy the multi-factor authentication request.

Hsu discloses this element. Ex-1003, ¶77. Hsu discloses that after the user provides the response (*i.e.*, “Palo Alto”) to the online account’s MFA request (*i.e.*, “In what city were you born?”), the information is then transmitted to the online account using the following command:

```

<?xml version="1.0" encoding="utf-8" ?> <cc:CCWSRequest
  xmlns:cc="http://www.intuit.com/CustomerCentral">
  <authentication><tp__
  partner_id>3</tp__partner_id><userId>
  ezQwQTgzNkIxLTdGRkItNDJBM
  C05RDc5LUJBOTc3MTcyMEY0NX0=</userId><password>X</
  password></authentication><body><ccreq:
  CCDiscoverAccountsInteractiveRequestxmlns:ccreq="http://
  www.intuit.com/CustomerCentral/Requests"><session>
  <cccaptureIpAddress>172.23.29.76</cccaptureIpAddress>
  <cccapturePort>9909</cccapturePort><ccscrapeIpAddress>
  172.23.29.76
  </ccscrapeIpAddress><ccscrapePort>9979</ccscrapePort>
  <ccscriptInstanceId>208666287<ccscriptInstanceId></
  session><answers
  >
  <answer>PaloAlto</answer></answers>
  </ccreq:CCDiscoverAccountsInteractiveRequest></body>
  </cc:CCWSRequest>AccountsInteractiveRequest</body>
  </cc:CCWSRequest>.

```

Ex-1004, [0035] (annotated).

Therefore, Hsu anticipates claim 1.

b) Claim 4

The method of claim 1, wherein the account holder's credentials are collected via a user interface.

Hsu discloses a user interface that collects the account holder/user's credentials. Ex-1003, ¶78; Ex-1004, [0040] (“The computer system 200 includes ... *a user interface 214* Moreover, the user interface 214 may include a display 216, a keyboard 218, and/or a pointer 220, such as a mouse”). The user interface in the Hsu system “receives the multiple authentication factors from the user,” which

include the account holder/user's credentials such as "usernames" and "passwords."

Id., [0029], [0047]. Therefore, Hsu anticipates claim 4.

c) Claim 5

The method of claim 1, wherein the account holder's credentials are collected from a data store.

Hsu discloses that the "authentication information from the user," which is account holder/user's credentials, is retrieved/collected from a "data structure 116," which is a data store. Ex-1003, ¶79; Ex-1004, [0031] ("The *information to be retrieved* may be initially stored locally on the computer 110 or remotely, for example, on the server 114, *in a data structure 116*"); [0035] ("The financial program may either request the authentication information (city of birth) from the user or may *retrieve the answer* (Palo Alto) *from storage*."); [0036] (same). Therefore, Hsu anticipates claim 5.

d) Claim 6

(1) [6pre]

A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

Hsu discloses [6pre]. *See supra* Claim 1, Element [1pre]; Ex-1003, ¶80.

(2) [6a]

collecting the account holder's credentials;

Hsu discloses [6a]. *See supra* Claim 1, Element [1a]; Ex-1003, ¶81.

(3) [6b]

encrypting the account holder's credentials using one or more processors;

Hsu discloses [6b]. *See supra* Claim 1, Element [1b]; Ex-1003, ¶82.

(4) [6c]

temporarily storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are held in memory;

Hsu discloses [6c]. *See supra* Claim 1, Element [1c]; Ex-1003, ¶¶83–84. Hsu discloses temporarily storing the account holder's encrypted credentials in memory. Ex-1004, [0041] (“Memory 224 in the computer system 200 may include *volatile memory and/or non-volatile memory*. More specifically, memory 224 may include ROM, RAM, EPROM, EEPROM, FLASH, one or more smart cards, one or more magnetic disc storage devices, and/or one or more optical storage devices.”); [0043] (“memory 224 includes optional stored information 244”); [0049] (“the system may optionally *store the multiple authentication factors* and/or the information”); [0039] (“stored authentication information ... are *encrypted*.”). Volatile memory, such as RAM, stores the account holder's credentials only temporarily. Ex-1003,

¶84; Ex-1010, 103 (“Nonvolatile memory retains its values when power is removed. Volatile memory loses its contents when power is removed. ... RAM is volatile.”).

(5) [6d]

verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;

Hsu discloses [6d]. *See supra* Claim 1, Element [1d]; Ex-1003, ¶85.

(6) [6e]

receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;

Hsu discloses [6e]. *See supra* Claim 1, Element [1e]; Ex-1003, ¶86.

(7) [6f]

prompting the account holder for a response and receiving the response thereto from the account holder; and

Hsu discloses [6f]. *See supra* Claim 1, Element [1f]; Ex-1003, ¶87.

(8) [6g]

transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Hsu discloses [6g]. *See supra* Claim 1, Element [1g]; Ex-1003, ¶88.

e) Claim 9

The method of claim 6, wherein the account holder's credentials are collected via a user interface.

Hsu discloses claim 9. *See supra* Claim 4; Ex-1003, ¶89.

f) Claim 10

The method of claim 6, wherein the account holder's credentials are collected from a data store.

Hsu discloses claim 10. *See supra* Claim 5; Ex-1003, ¶90.

B. Ground 2: Anticipation by Hazlehurst (Claims 1, 4–6, and 9–10)

1. Summary of Hazlehurst (Ex-1005)

Hazlehurst is directed to “systems and methods for gathering summary data and authorizing Web transactions.” Ex-1005, 1:14–16. Hazlehurst explains that the recent developments of “Web token generators” and “CAPTCHA” beyond the traditional username/password credentials present a challenge for automated proxy services, because the existing technology “has no way of inputting or utilizing the unique user token data without the user’s direct input.” *Id.*, 1:53–2:29.

To address this challenge, Hazlehurst discloses a system that leverages “at least two of the authentication form factors.” *Id.*, 2:39–41. These factors include: “(1) Something a person knows, such as a password, a PIN or an out-of-wallet-response. (2) Something a person has, such as a mobile phone, a credit card or a

hardware security token. (3) Something a person is, such as represented by a fingerprint, by a retinal scan, or by some other biometric.” *Id.*, 2:30–2:38.

As shown in Figure 1, the system includes a portal server (PS) 105 that can log in, using credentials stored in an encrypted user pin vault (UPV) file 113, to access data in servers 104 or 109 and perform transactions on behalf of a user. *Id.*, 4:37–42, 4:61–65.

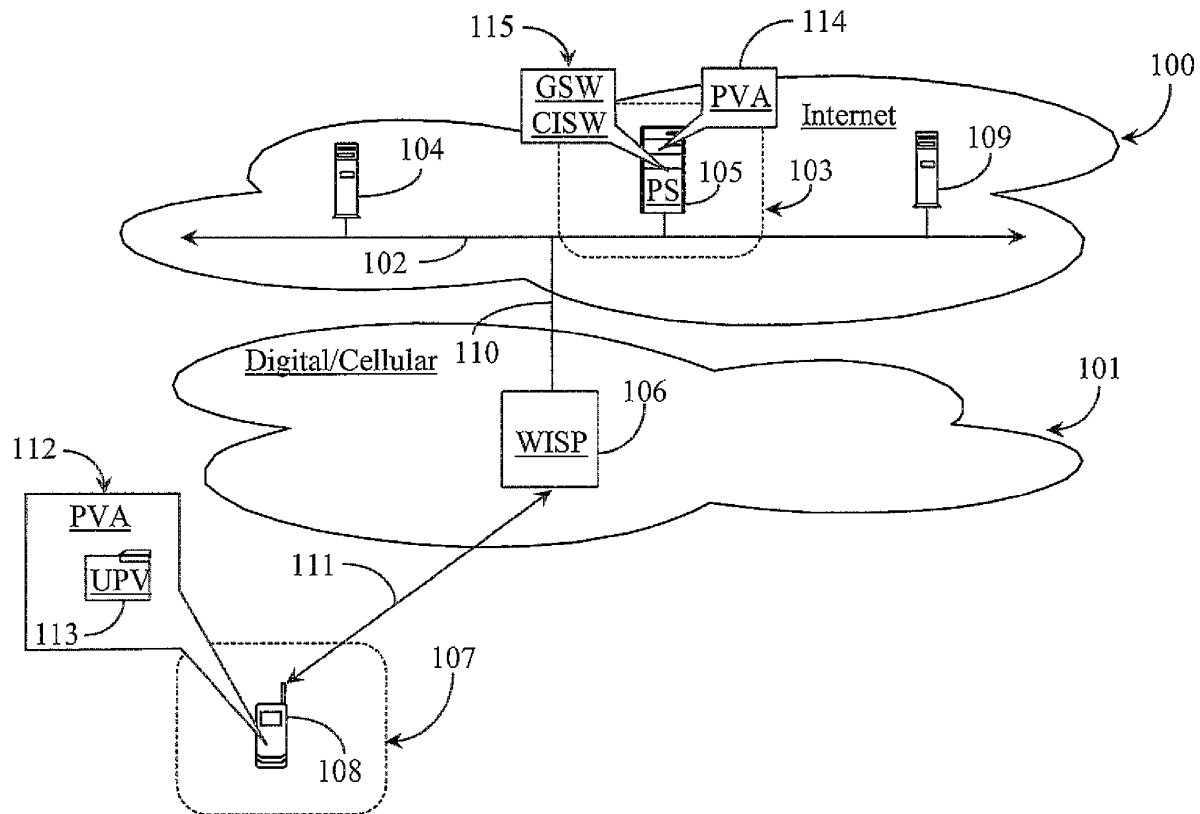


Fig. 1

Id., Fig. 1.

2. Detailed Analysis of Ground 2

a) Claim 1

(1) [1pre]

Hazlehurst discloses this element. Ex-1003, ¶¶96–100. Hazlehurst discloses a “**Pin Vault Application**” (*i.e.*, third-party entity) that can access “**a Web-based account**” (*i.e.*, online account) that requires account holder/user’s credentials for login (*i.e.*, secured by MFA). Ex-1005, Abstract (“**the Pin Vault software** cooperates with an Internet service to provide, from the Pin Vault, data as needed by the Internet service to **log onto and authenticate as the user at the one or more web sites** storing information of interest to the user, to gather information on behalf of the user.”); 1:59–61 (“**a Web-based account** or service may **require the user to log in and provide, in addition to normal user credentials, a token that changes in value, say every 60 seconds.**”). The user in Hazlehurst is an account holder, because the user “subscribes to services offered by service provider,” *id.*, 4:7–9, and later provides “user credentials” to log in the “Web-based account or service.” *Id.*, 1:59–61.

Hazlehurst’s accessing method is done in a secure manner, because the “authentication credentials” stored in the Pin Vault are “**encrypted**” and the Pin Vault application has an “**encryption/decryption software (SW)** to decrypt and use

the user authentication credentials” from the Pin Vault to access the Web-based account. *Id.*, 4:48–67.

Hazlehurst also discloses that the online account is secured by a “**two-factor authentication**” protocol, such as “**time sensitive tokens**” and “**CAPTCHA.**” *Id.*, 5:30–34 (“In an embodiment where **one or more sites use time sensitive tokens as part of the two-factor authentication**, PS 105 may obtain the correct token file from device 108 at the same time the standard authentication credentials are obtained at the time of login to the site.”); 5:38–43 (In the case that **any of the user’s sites require submission of CAPTCHA data**, those CAPTCHA displays, including the appropriate data entry boxes, may be captured from those sites and then submitted to device 108 at which time the user operating the device may type in the appropriate characters required by the site as part of the **two-factor authentication.**”).

(2) [1a]

Hazlehurst discloses this element. Ex-1003, ¶¶101–02. Hazlehurst discloses that the Pin Vault Application (PVA) must “obtain” the account holder/user’s credentials from the user. *Id.*, 8:42–44 (“the user has the **required credentials** stored locally on his or her device and **the system must obtain them from the user**”); 4:48–52 (“the client-side PVA application 112 contains an encrypted user pin vault (UPV) file 113 that is adapted to store at minimum all of the **user’s** subscribed-to Web site locations and appropriate **authentication credentials** for accessing those sites”);

1:42–45 (“[A]utomatic logins are accomplished for a subscriber at Internet destinations by use of *pre-stored* configuration information and *user authentication credentials*.”). A portal server 105 can also collect the account holder/user’s credentials submitted by the account holder/user. *Id.*, 5:15–18 (“In applications ... without PVA 114 or 112, the user submits the required Web site access and authentication data to PS 105 for storage.”).

The collected MFA factors (*i.e.*, account holder’s credentials) may include: “(1) Something a person knows, such as a password, a PIN or an out-of-wallet-response. (2) Something a person has, such as a mobile phone, a credit card or a hardware security token. (3) Something a person is, such as represented by a fingerprint, by a retinal scan, or by some other biometric.” *Id.*, 2:30–38.

113

My Pin Vault			
201	202	203	204
<u>URL</u>	<u>User Name</u>	<u>PIN/Password</u>	<u>Token File</u>
*****	**** *	*****	
*****	**** *	****	
*****	**** *	*****	
*****	**** *	**** *	
*****	**** *	*****	

Fig.2

Id., Fig. 2 (annotated).

(3) [1b]

Hazlehurst discloses this element. Ex-1003, ¶¶103–04. Hazlehurst discloses that “the client-side PVA application 112 contains *an encrypted user pin vault (UPV) file 113* that is adapted to store at minimum all of the *user’s* subscribed-to Web site locations and appropriate *authentication credentials* for accessing those sites.” Ex-1005, 4:48–52; 4:65–67 (“PVA 114 has the appropriate encryption/decryption software (SW) to decrypt and use the user authentication credentials from UPV 113.”).

The account holder/user’s credentials are encrypted by PVA 112 on device 108. *Id.*, 5:20–22 (“Provision of PVA 112 on device 108 enables the user to keep the sensitive information stored locally in encrypted format.”); 4:19–23 (“device 108 is a personal handheld device ... Device 108 may also be a PDA, a laptop computer, or a desktop computer”). That device 108 “enables” the storage of information in encrypted format means the encryption is an “other operation[]” performed by one or more processors on the device 108. Ex-1003, ¶104; Ex-1010, 39 (“Calculations and other operations in your program are performed by a central processing unit (CPU) inside the computer.”); *id.*, 18 (“Most modern computer systems provide more than one CPU (or ‘core’) within the computer system.”). That encryption software “running on PS 105” means it is executed by one or more processors on portal server 105. Ex-1003, ¶104; Ex-1005, 4:58–59.

(4) [1c]

Hazlehurst discloses this element. Ex-1003, ¶¶105–06. Specifically, Hazlehurst discloses “*a Pin Vault file stored in a data repository*” where the Pin Vault file comprises “data for authenticating the user to one or more web sites,” which means that the account holder/user’s credentials are stored in a data store. Ex-1005, 2:53–59; 5:15–18 (“In applications ... without PVA 114 or 112, the user submits the required Web site access and authentication data to PS 105 for storage.”). The Pin Vault file that contains the account holder/user’s credentials is “*encrypted*.”

Id., 4:48–50 (“the client-side PVA application 112 contains an encrypted user pin vault (UPV) file 113”).

The Pin Vault file is stored using one or more processors on device 108, such as a cell phone, PDA, PC, or laptop computer. *Id.*, 4:52–56 (“UPV file 113 may be a small file downloadable to a cell phone, PDA, or other device Likewise, the UPV file may be stored locally on any PC or laptop computer.”); 5:20–22 (“Provision of PVA 112 on device 108 enables the user to keep the sensitive information stored locally in encrypted format.”). Storage is an “other operation[]” that is described as being performed by one or more processors on the device. Ex-1003, ¶106; Ex-1010, 39 (“Calculations and other operations in your program are performed by a central processing unit (CPU) inside the computer.”); *id.*, 18 (“Most modern computer systems provide more than one CPU (or ‘core’) within the computer system.”).

(5) [1d]

Hazlehurst discloses this element. Ex-1003, ¶107. Hazlehurst discloses a system where “**PS [(portal server)] 105** may navigate to various user-subscribed Web sites and ... **may log in representing the user and access specific data from those sites** and even perform certain transactions at those sites, authorized by the user.” Ex-1005, 4:37–42. This login process involves “**authenticating as the user using authentication data**” (*i.e.*, verifying the account holder’s credentials ... using

account holder's credentials). *Id.*, 3:25–26; 9:16–20 (In an embodiment where CAPTCHA is required, “one [software] transaction is used to submit the CAPTCHA data and the username password/PIN credential to the gatherer”, and then “the gatherer agent uses the credentials and the CAPTCHA data to authenticate the user.”). As discussed above, the “Web-based account” being accessed in Hazlehurst is an online account that requires account holder/user credentials. *Id.*, Abstract, 1:59–61

This verification/access process is running by one or more processors on a portal server (*e.g.*, PS 105 in Hazlehurst). Ex-1003, ¶108; Ex-1005, 5:27–30 (“PS 105 aided by PVA 114 may access device 108 as needed and interrogate UPV 113 to obtain required site location information and authentication data needed to access the sites.”); Ex-1010, 77 (“In a client-server configuration, a program on a client computer accepts services and resources from a complementary program on a server computer.”); Ex-1010, 39 (“Calculations and other operations in your program are performed by a central processing unit (CPU) inside the computer.”); Ex-1010, 44 (“Most modern computer systems provide more than one CPU (or ‘core’) within the computer system.”).

(6) [1e]

Hazlehurst discloses this element. Ex-1003, ¶¶109–12. Hazlehurst discloses that the system receives a MFA request in the form of a “token” or “CAPTCHA”

from the “Web-based account.” Ex-1005, 1:59–62 (“a *Web-based account or service* may *require the user to log in and provide*, in addition to normal user credentials, *a token* that changes in value, say every 60 seconds.”); 5:38–43 (“In the case that any of the *user’s sites require submission of CAPTCHA data*, those CAPTCHA displays, including the appropriate data entry boxes, may be captured from those sites and then submitted to device 108 at which time the user operating the device may type in the appropriate characters required by the site as part of the two-factor authentication.”). Hazlehurst provides in Figure 5 “a two-factor authentication sequence by proxy leveraging CAPTCHA input.” *Id.*, 3:44–46.

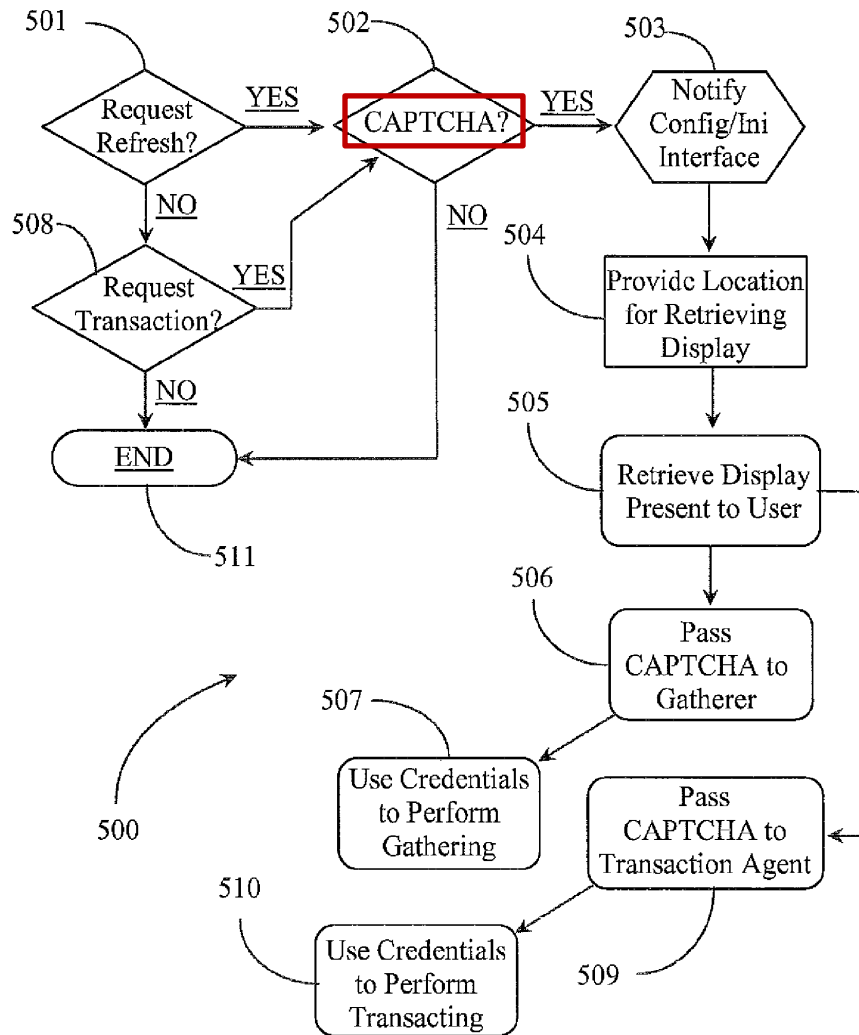


Fig. 5

Id., Fig. 5 (annotated). The account holder/user’s response to the MFA request is required before further access to the online account is granted, because the system “need[] to obtain the required data in order to access the appropriate Web sites and services,” *id.*, 4:61–65, and if “the credentials fails then the system may automatically reattempt the sequence.” *Id.*, 8:28–31.

(7) [1f]

Hazlehurst discloses this element. Ex-1003, ¶¶113–14. Hazlehurst discloses that if the system receives a MFA request in the form of CAPTCHA, it prompts the account holder/user for a response by “*present[ing] the [CAPTCHA] display to the device of the user along with the appropriate data entry box or field for the user to type in the required characters.*” Ex-1005, 9:2–6; 5:38–43 (“In the case that any of the user’s sites require submission of CAPTCHA data, those CAPTCHA displays, including the appropriate data entry boxes, may be captured from those sites and then *submitted to device 108* at which time the user operating the device may type in the appropriate characters required by the site as part of the two-factor authentication.”). The system then receives the MFA response “submitted” by the account holder/user at the time of login attempt, in order to “retrieve the user login credentials and accept the user-submitted CAPTCHA data in the same transaction.” *Id.*, 5:44–47.

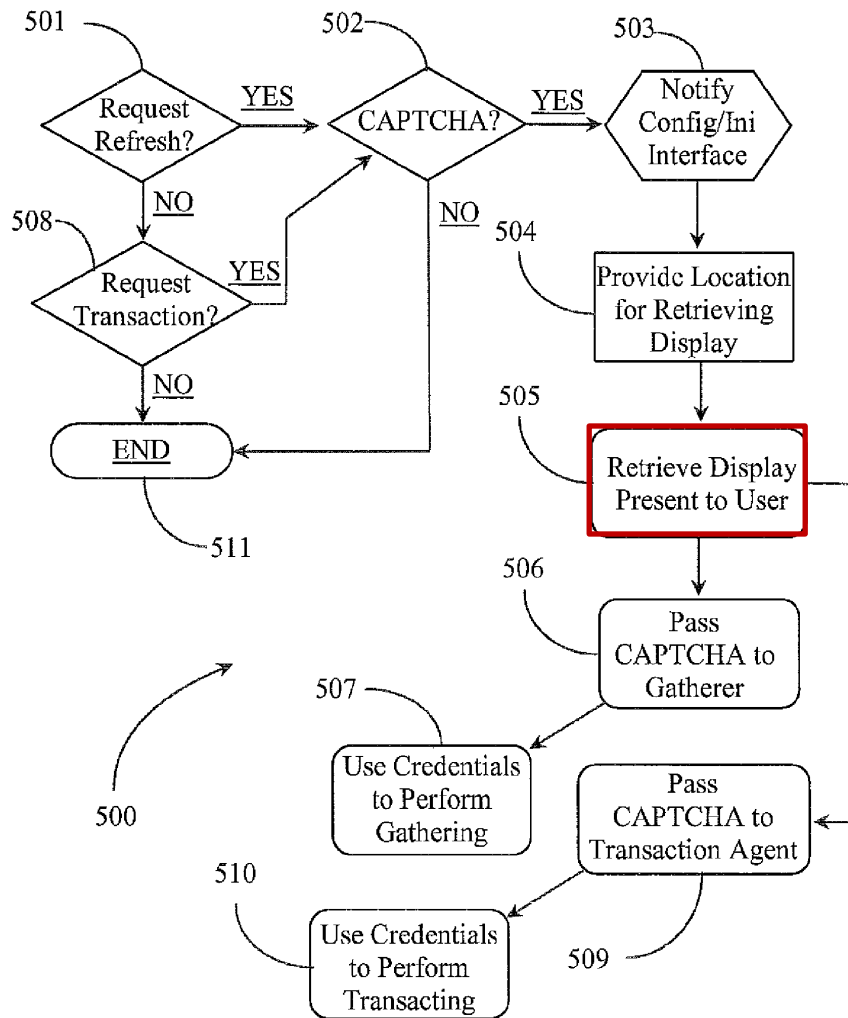


Fig. 5

Id., Fig. 5 (annotated).

(8) [1g]

Hazlehurst discloses this element. Ex-1003, ¶115. Hazlehurst discloses a “gatherer agent” (*i.e.*, third-party entity) that transmits the account holder/user’s MFA response (*e.g.*, CAPTCHA) to the “Web-based account” in order to satisfy the MFA request. Ex-1005, 5:3–7 (“PS 105 in addition to PVA 114, has a gatherer software (GSW) agent application 115 ... that may spawn multiple individual instances for performing ... site login authentication”); 9:19–20 (“*[T]he gatherer agent uses the credentials and the CAPTCHA data to authenticate the user in step 507.*”); 1:59–62, 2:12–14 (“[A] Web-based account or service may require the user to log in and provide, in addition to normal user credentials, a token that changes in value, say every 60 seconds” and “may be configured to initiate the CAPTCHA whenever a request for services is received.”).

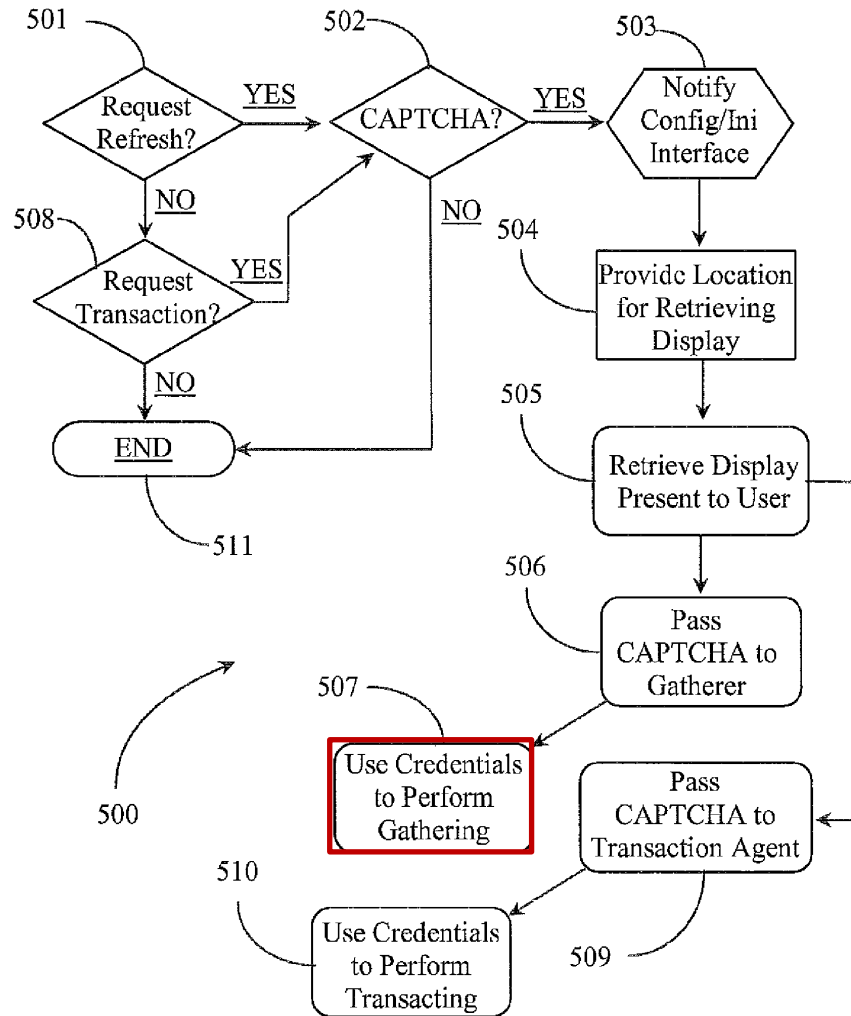


Fig. 5

Id., Fig. 5 (annotated).

Therefore, Hazlehurst anticipates claim 1.

b) Claim 4

Hazlehurst discloses this element. Ex-1003, ¶¶116–17. Specifically, Hazlehurst discloses a “*pin vault user interface (UI)*” that “may be an integral part

of PVA,” the Pin Vault Application. Ex-1005, 6:64–67. Hazlehurst further explains that “PVA 112 contains an encrypted user pin vault (UPV) file 113 that is adapted to store at minimum all of the *user’s ... authentication credentials* for assessing those sites.” *Id.*, 4:48–52. UPV file 113 “*may ... be displayable* and may vary widely in displayed.” Ex-1005, 6:14–19.

113

<u>My Pin Vault</u>	<u>URL</u>	<u>User Name</u>	<u>PIN/Password</u>	<u>Token File</u>
	*****	**** *	*****	
	*****	**** *	****	
	*****	**** *	*****	
	*****	**** *	*****	
	*****	**** *	*****	

Fig.2

Id., Fig. 2. Figure 2 shows how the PVA user interface (UI) collects the account holder/user’s credentials, including “User Name[s],” “PIN/Password[s],” and “Token File[s].” *Id.*, 6:20–32, 6:39–44. Therefore, Hazlehurst anticipates claim 4.

c) Claim 5

Hazlehurst discloses this element. Ex-1003, ¶118. For example, Hazlehurst discloses that a “Pin Vault file,” which contains the account holder/user’s credentials, is stored in a “data repository,” which is a data store. Ex-1005, 2:56–59 (“*a Pin Vault file stored in a data repository* coupled to the appliance, the Pin Vault file comprising data for authenticating the user to one or more web sites storing information of interest to the user.”). Further, Hazlehurst discloses that PS 105 collects the account holder’s credentials from the data repository by “*access[ing] UPV 113*” (*i.e.*, the Pin Vault file) on the user’s device when needed to “obtain the required data in order to access the appropriate Web sites and services.” *Id.*, 4:61–65. Therefore, Hazlehurst anticipates claim 5.

d) Claim 6

(1) [6pre]

Hazlehurst discloses [6pre]. *See supra* Claim 1, Element [1pre]; Ex-1003, ¶119.

(2) [6a]

Hazlehurst discloses [6a]. *See supra* Claim 1, Element [1a]; Ex-1003, ¶120.

(3) [6b]

Hazlehurst discloses [6b]. *See supra* Claim 1, Element [1b]; Ex-1003, ¶121.

(4) [6c]

Hazlehurst discloses temporarily holding the account holder/user’s encrypted credentials in memory using one or more processors. Ex-1003, ¶¶122–23. Hazlehurst discloses that PS 105 (*e.g.*, third-party entity) “temporar[ily] stor[es]” the account holder/user’s UPV data. Ex-1005, 5:63–65 (“[A] user may also elect to transmit some or all of their UPV data to PS 105 for permanent or **temporary storage**.”). The UPV data is temporarily stored using one or more processors on the portal server (*e.g.*, PS 105). *See supra* Element [1c]; Ex-1003, ¶106.

Hazlehurst further discloses an embodiment where “PS 105 does not retain any user authentication information locally.” *Id.*, 4:60–61. Instead, “when PS 105 is performing ... services for the user, it accesses UPV 113 from the user’s device when needed to obtain the required data in order to access the appropriate Web sites and services.” *Id.*, 4:61–65. PS 105 then temporarily holds the UPV 113 in its memory for the “encryption/decryption software (SW) to decrypt and use the user authentication credentials from UPV 113.” *Id.*, 4:65–67.

(5) [6d]

Hazlehurst discloses [6d]. *See supra* Claim 1, Element [1d]; Ex-1003, ¶124.

(6) [6e]

Hazlehurst discloses [6e]. *See supra* Claim 1, Element [1e]; Ex-1003, ¶125.

(7) [6f]

Hazlehurst discloses [6f]. *See supra* Claim 1, Element [1f]; Ex-1003, ¶126.

(8) [6g]

Hazlehurst discloses [6g]. *See supra* Claim 1, Element [1g]; Ex-1003, ¶127.

e) Claim 9

Hazlehurst discloses claim 9. *See supra* Claim 4; Ex-1003, ¶128.

f) Claim 10

Hazlehurst discloses claim 10. *See supra* Claim 5; Ex-1003, ¶129.

C. Ground 3: Obviousness Over Emerson in view of Hsu (Claims 1, 4–6, and 9–10)

1. Summary of Emerson (Ex-1006)

Emerson discloses “a method for conducting a secure transaction over a network,” specifically, a method that “facilitates electronic fund transfers, initiated at a merchant site, from a consumer’s financial institution to the merchant.” Ex-1006, [0001], [0010]. The method can be implemented through a system illustrated in Figure 1, which includes a merchant server 104, a financial institution server 106, an online debit system (ODS) server 108 running an ODS agent 114, and the consumer 110, all connected over the Internet 112. *Id.*, [0035].

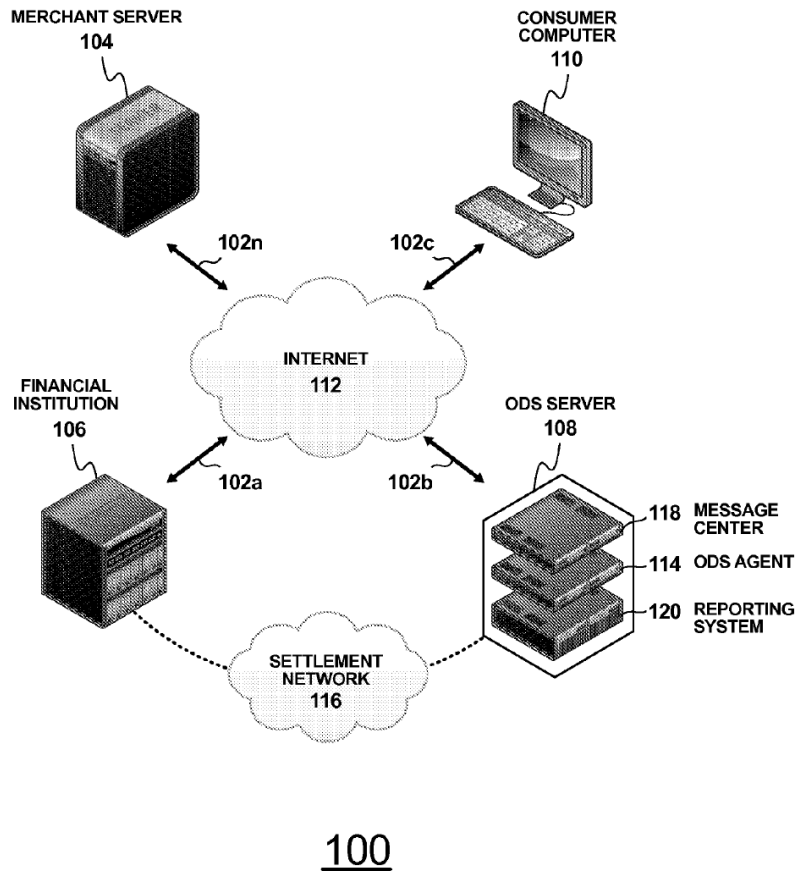
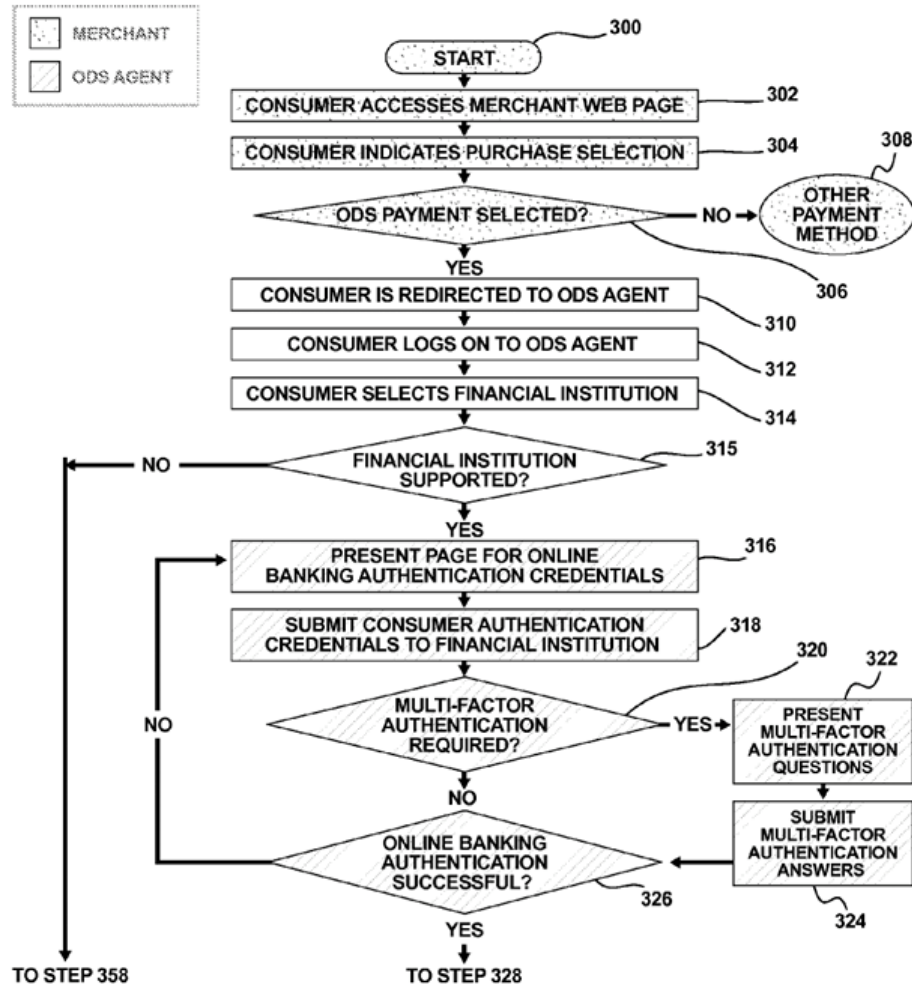


FIG. 1

Id., Fig. 1.

Emerson further explains that “[m]ost banks nowadays require multi-factor authentication” which involves “usual authentication credentials such as log-in and password” and “(random) Q and A (question and answer) tests from a set of questions that are preset by a consumer for on-line banking.” *Id.*, [0059]. To address the MFA request, Emerson discloses that the ODS agent 114 determines the information required by the bank for gaining access to the consumer’s account,

requests authentication credentials and MFA information from the consumer, and submits the information to the bank. *Id.*, [0069]–[0072].



300

FIG. 3a

Id., Fig. 3a.

2. Motivation to Combine Emerson and Hsu

A POSITA would have been motivated to combine Emerson and the encryption technique disclosed in Hsu, and would have had a reasonable expectation of success in doing so. Ex-1003, ¶¶139–42.

Emerson and Hsu are extraordinarily similar. Fundamentally, they identify the same problem—the use of MFA in authenticating online account holders makes it difficult for third-party automated systems to securely and unattended access the accounts, as MFA typically requires direct user input. Ex-1003, ¶140; Ex-1004, [0004]; Ex-1006, [0075]. And both propose similar solutions to address this problem—using a third-party system that collects the account holder’s credentials and MFA responses, enabling automated access to the accounts. Ex-1003, ¶140; Ex-1004, [0023]; Ex-1006, Fig. 3a. Therefore, a POSITA looking to implement the account access method in Emerson would have looked at other similar methods, such as Hsu, to enhance security and automation. Ex-1003, ¶140.

Specifically, Emerson and Hsu both recognize that the information being processed by the system (such as authentication credentials and financial information) is “sensitive” in nature, Ex-1004, [0039]; Ex-1006, [0032], and that “security” of transactions is a major issue in online banking. Ex-1004, [0003], [0005]; Ex-1006, [0032]. Emerson also emphasizes repeatedly that the method is for conducting a “secure” transaction over a network. Ex-1006, Abstract, [0010],

[0014], [0015], [0031], [0047], [0053], claims 1, 8, 14, 18. Thus, a POSITA seeking to implement the method disclosed in Emerson would have been motivated to look for available methods, like in Hsu, to find a way to further enhance its security. Ex-1003, ¶141.

Hsu teaches a way to enhance security of the MFA banking process through encryption. Ex-1004, [0039]. Hsu further discloses two complementary ways to use encryption: (1) encrypting the information and storing it locally on a computer or remotely on a server, *id.*, [0026], [0029], [0031], [0039], [0043], and (2) encrypting the information when it is communicated over the network. *Id.*, [0039]. A POSITA would have understood that encrypting sensitive information would have been beneficial because it can avoid exposing the information to malicious actors on the Internet. Ex-1003, ¶141. Therefore, a POSITA would have been motivated to add encryption, as taught by Hsu, to the verification process in Emerson to address the well-known security threat of using unencrypted information. Ex-1003, ¶141.

Furthermore, a POSITA would have had a reasonable expectation of success in incorporating encryption of Hsu into the method disclosed in Emerson. Ex-1003, ¶142. Emerson's system already has a "processor" operable to receive input from the user and communicate with financial institutions. Ex-1006, [0014]. This processor can be easily programmed by a POSITA to encrypt the account holder's

credentials or other information when communicated with financial institutions, as taught by Hsu. Ex-1003, ¶142; Ex-1004, [0039].

3. Detailed Analysis of Ground 3

a) Claim 1

(1) [1pre]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶135–38. Specifically, Emerson discloses a third-party entity termed “**ODS agent 114**” which “acts independently based on a pre-determined set of steps and interactions necessary to complete a bill pay or other payment on behalf of the consumer” and is “bank independent,” *i.e.*, “no ‘system-level’ or dependent integration with any bank or any specific financial system.” Ex-1006, [0075], [0090]. The ODS agent provides “**on-line banking authentication and fund transfer services through a specific financial institution.**” *Id.*, [0053]. For on-line banking authentication, “**the ODS agent 114** determines the information required by the selected financial institution for **gaining access to the consumer’s account at the institution.**” *Id.*, [0069].

Further, Emerson discloses that the “**ODS agent 114** ... implements on-line banking authentication” through “cach[ing] (device) tokens set by on-line banking to pass **multi-factor authentication** when applicable.” Ex-1006, [0060]. In another embodiment, “the **ODS agent 114** determines whether or not the financial institution

106 requires ‘**multi-factor authentication**.’ *Id.*, [0070]. If the answer is yes, “the **ODS agent 114** presents the **multi-factor authentication** to the consumer,” and “submits the consumer’s answer to the financial institution 106.” *Id.*, [0071].

In addition, Hsu discloses that the access is gained in a secure manner, as the “stored authentication information and/or stored retrieved information are **encrypted**” and “may be **encrypted** when it is communicated over the network.” Ex-1004, [0039]. As discussed above, a POSITA would have been motivated to combine Emerson’s ODS agent with Hsu’s encryption technique, and would have had a reasonable expectation of success in doing so. Ex-1003, ¶¶139–42.

(2) [1a]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶143–44. As shown in Figure 6, Emerson teaches that the ODS agent 114 presents a financial institution log-in information page (*e.g.*, page 600) to the consumer and requests authentication credentials (*e.g.*, user ID 601 and password 604) from the consumer. Ex-1006, [0069]. After the consumer hits the “next” button 606, the ODS agent collects the information and submits it to the financial institution. *Id.*

eMerchant Demo

Your Purchase	Pay To: eMerchant Demo
	Amount: \$ 1.25 USD

Sign in to your Bank ABC online banking to approve your purchase.

User ID:
Password:

Next

[Choose a different bank](#)

[Return to Merchant](#)

[Have Questions?](#)

600

FIG. 6

Id., Fig. 6 (annotated).

(3) [1b]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶145–46. Hsu teaches encrypting the account holder’s credentials. Ex-1004, [0039] (“The multi-factor authentication information ... are *encrypted*. In addition, such information may be *encrypted* when it is communicated over the network 112.”).

The information is encrypted by the “encryption module” using “one or more processing units.” *Id.*, [0043]–[0044] (“memory 224 includes ... optional ***encryption module*** (or a set of instructions) 250. ... Instructions in the various modules in the memory 224 may be implemented in a high-level procedural language, an object-oriented programming language, and/or in an assembly or machine language. The programming language may be compiled or interpreted, i.e., configurable or configured to be ***executed by the one or more processing units 210.***”). As discussed above, a POSITA would have been motivated to apply Hsu’s encryption technique to encrypt the collected user ID 602 and password 604 in Emerson, and would have had a reasonable expectation of success in doing so. Ex-1003, ¶¶139–42, 146.

(4) [1c]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶147–48. Emerson discloses that the ODS agent 114 may “***cache (device) tokens*** set by on-line banking to pass multi-factor authentication” and “***stor[e] it in a database for subsequent usage.***” *Id.*, [0060].

Furthermore, Emerson discloses that the consumer’s personal information is stored at the “ODS server 108” using one or more “processors 202 or 204,” in order to compare it with the information submitted by merchant. Ex-1006, [0066] (“[T]he consumer’s personal information can be provided to the ODS server 108 by the merchant server 104. In one embodiment, as a security measure, the ODS agent 114

asks for the same information and compares it to that submitted by the merchant server 104. If a difference in the two sets of information is detected, the transaction may be declined.”). Emerson explains that the ODS server 108 “may be a symmetric multiprocessor (SMP) system including a plurality of *processors 202 and 204*” and “[t]he *processor 202 or 204* in conjunction with memory controller 208 controls what data is stored in memory 209.” *Id.*, [0040].

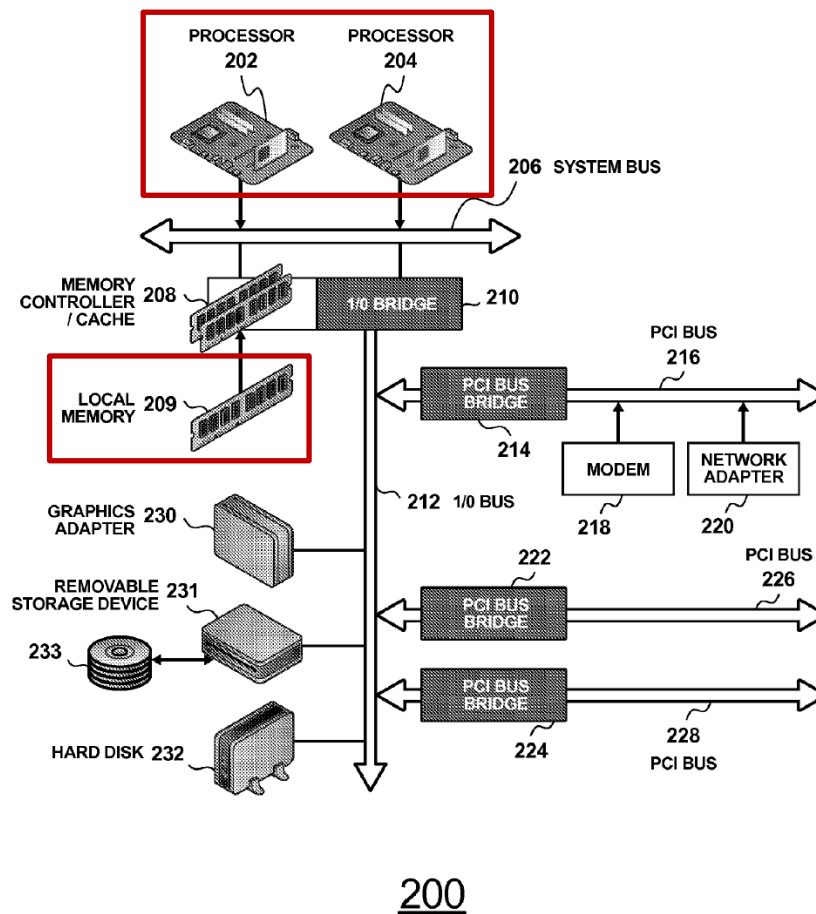


FIG. 2

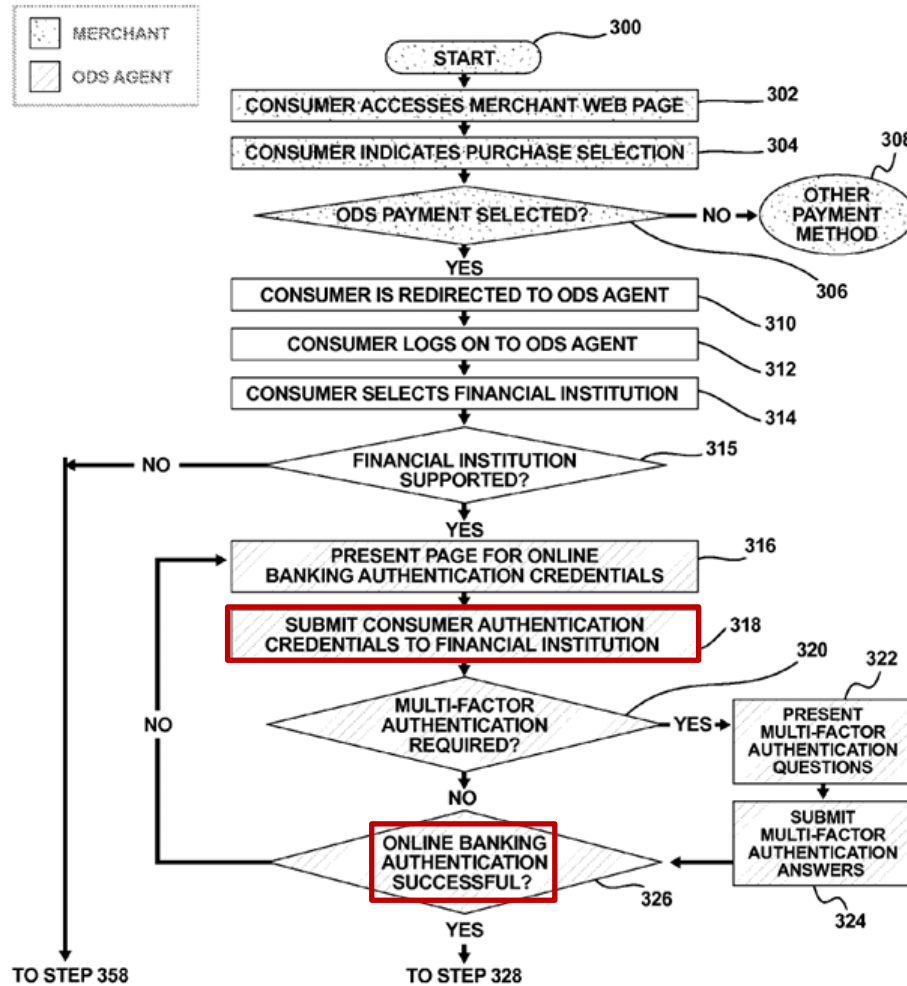
Id., Fig. 2 (annotated).

Hsu also teaches storing the account holder's encrypted credentials in a data store. *See supra* Ground 1, Claim 1, Element [1c]. It would have been obvious to a POSITA to store the collected information (*e.g.*, user ID 602 and password 604 in Emerson) at the ODS server, because Emerson seeks to overcome the lack of “built in identity verification” by using the ODS agent to “automatically perform[] substantially all steps for electronic communication with a financial institution to gain access to an account.” Ex-1003, ¶148; Ex-1006, [0011]. A POSITA would have had a reasonable expectation of success in incorporating Hsu's stored credentials technique in the Emerson system, because Emerson discloses a similar technique where a type of authentication credentials (*e.g.*, token) is stored in a database for subsequent usage. Ex-1003, ¶148; Ex-1006, [0060].

(5) [1d]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶149–50. Emerson discloses that the ODS agent 114 collects the account holder's credentials, such as user ID 602 and password 604. *See supra* Element [1a]. After the account holder's credentials are collected, the ODS agent 114 “implements *on-line banking authentication*” by submitting “*the information contained in the fields 602 and 604 ... to the specified financial institution in step 318.*” Ex-1006, [0069]. If the financial institution accepts the authentication credentials (step 326) (in other words verifies those credentials), “*the ODS agent 114 acts on behalf of the consumer and*

maintains a session with the financial institution 106 in order to interact and respond to actions and messages from the financial institution 106,” i.e., accessing the online account using the account holder’s credentials. Id., [0072]–[0073].



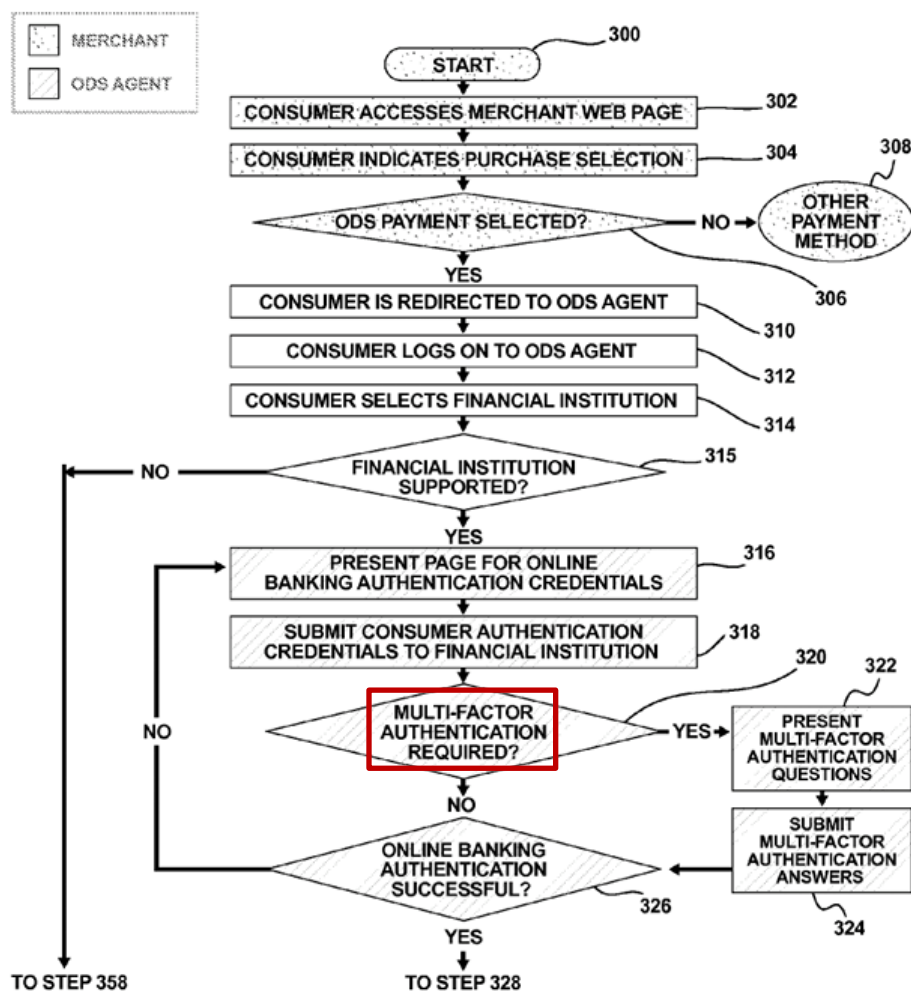
300

FIG. 3a

Id., Fig. 3a (annotated). This verification/access process is completed using one or more processors 202 and/or 204. *Id.*, [0044] (“the computer programs, when executed, enable the ***processor 202 and/or 204*** to perform the features of the ODS agent 114”); Ex-1003, ¶150.

(6) [1e]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶151. Emerson discloses receiving a MFA request specifically where it states that “[i]n step 320, the ODS agent 114 determines whether or not ***the financial institution 106 requires ‘multi-factor’ authentication.***” Ex-1006, [0070]. That passage explains that a response to the MFA is required from the account holder before access to the online account is granted. *Id.*; [0072] (“If the customer is unable to enter the correct authentication credentials the transaction will not proceed.”). Emerson describes user-selected graphics or challenge questions as examples of additional MFA factors that can be used for granting (or denying) account access. *Id.*, [0059], [0070].



300

FIG. 3a

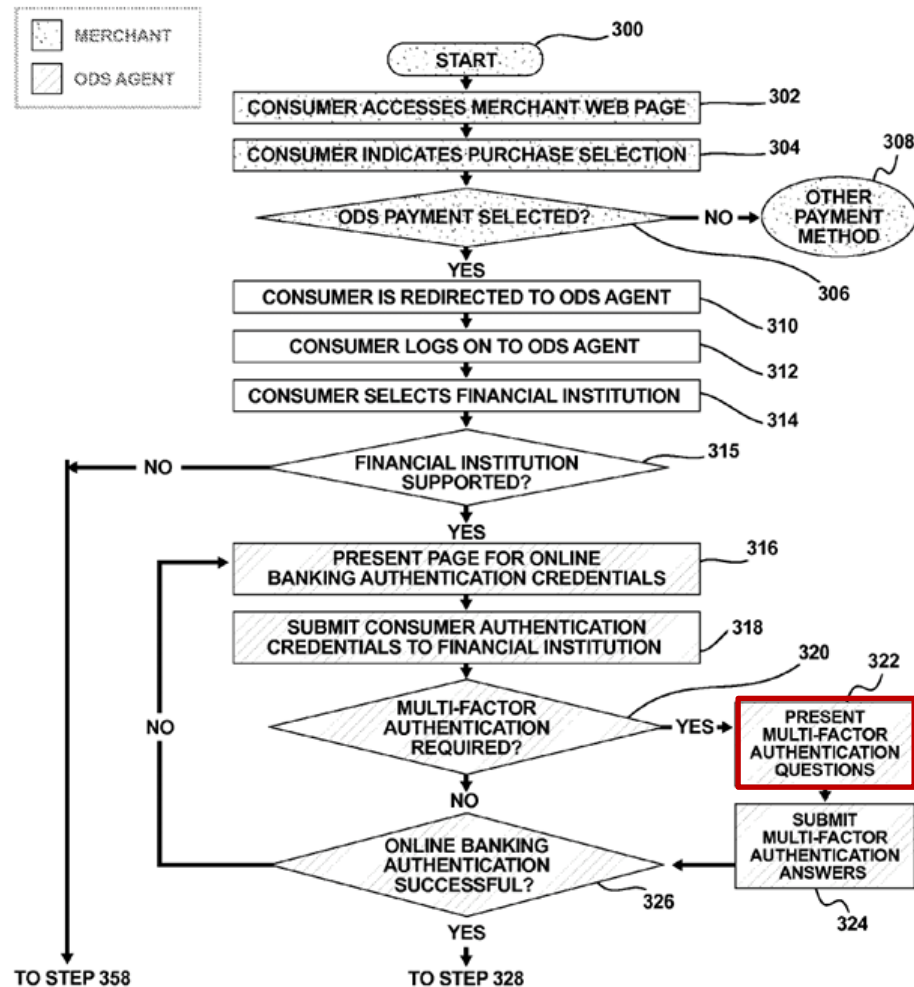
Id., Fig. 3a (annotated).

(7) [1f]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶152.

Emerson discloses that if MFA is required in step 320, “the process moves to step

322 where *the ODS agent 114 presents the multi-factor authentication to the consumer*” (the consumer is the account holder in Emerson) and then “[t]he consumer presents the answer” to the ODS agent 114. Ex-1006, [0071].



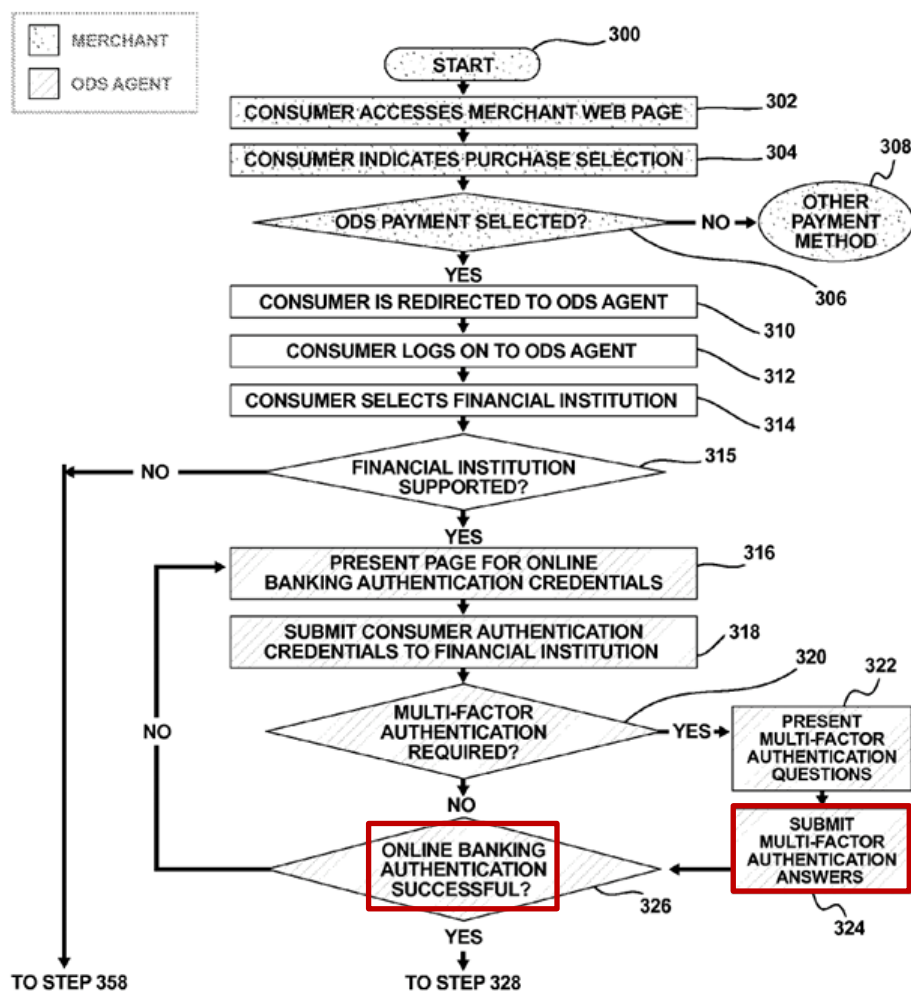
300

FIG. 3a

Id., Fig. 3a (annotated).

(8) [1g]

The Emerson/Hsu combination discloses this element. Ex-1003, ¶153. Emerson discloses that after receiving the answer to the MFA request from the account holder/consumer, “*the ODS agent 114 submits the consumer’s answer to the financial institution 106.*” Ex-1006, [0071]. “*In step 326, the ODS agent 114 interprets the response from the financial institution and determines whether the authentication credentials are valid and accepted by the financial institution.*” *Id.*, [0072]. “If the authentication credentials are accepted by the financial institution ..., the ODS agent 114 acts on behalf of the consumer and maintains a session with the financial institution 106 in order to interact and respond to actions and messages from the financial institution 106.” *Id.*, [0073].



300

FIG. 3a

Id., Fig. 3a (annotated).

Therefore, the Emerson/Hsu combination renders Claim 1 obvious.

b) Claim 4

The Emerson/Hsu combination renders this claim obvious. *See supra* Claim 1, Element [1a]; Ex-1003, ¶154. Specifically, Figure 6 in Emerson presents a user interface termed “page 600” that is used to collect the account holder’s credentials, such as user ID 602 and password 604. Ex-1006, [0069] (“ODS agent 114 ... presents a financial-institution log-in information page, such as page 600, to the consumer.”).

eMerchant Demo

Your Purchase

Pay To: eMerchant Demo
Amount: \$ 1.25 USD

Sign in to your Bank ABC online banking to approve your purchase.

User ID:

Password:

[Choose a different bank](#)

[Return to Merchant](#)

[Have Questions?](#)

600

FIG. 6

Id., Fig. 6.

c) **Claim 5**

The Emerson/Hsu renders claim 5 obvious. Ex-1003, ¶¶155–56. Emerson discloses using the account holder’s credentials stored in a data store for authentication. *See supra* Claim 1, Element [1c]; Ex-1006, [0060] (“ODS agent 114 ... implements on-line banking authentication. It may ***cache (device) tokens set by on-line banking to pass multi-factor authentication*** when applicable. The caching mechanism may be implemented by keeping track of the token for a specific on-line banking log-in and ***storing it in a database for subsequent usage.***”).

Hsu also discloses retrieving/collecting the account holder’s credentials from a data store. *See supra* Ground 1, Claim 5, Element [1c]. Ex-1004, [0035] (“The financial program may ... ***retrieve the answer (Palo Alto) from storage.***”). It would have been obvious to a POSITA to store the collected information (*e.g.*, user ID 602 and password 604 in Emerson) at the ODS server and later collect this information from the ODS server for automatic login, because Emerson seeks to overcome the problem of not having “built in identity verification” by using the ODS agent to “automatically perform[] substantially all steps for electronic communication with a financial institution to gain access to an account.” Ex-1003, ¶156; Ex-1006, [0011]. A POSITA would have had a reasonable expectation of success in incorporating Hsu’s stored credentials technique in the Emerson system, because Emerson

discloses a similar technique where a type of authentication credentials (*e.g.*, token) is stored in a database for subsequent usage. Ex-1003, ¶156; Ex-1006, [0060].

d) Claim 6

(1) [6pre]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1pre]; Ex-1003, ¶157.

(2) [6a]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1a]; Ex-1003, ¶158.

(3) [6b]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1b]; Ex-1003, ¶159.

(4) [6c]

The Emerson/Hsu combination teaches this element. Ex-1003, ¶¶160–63. Emerson discloses that the ODS agent 114 may “*cache (device) tokens* set by on-line banking to pass multi-factor authentication.” Ex-1006, [0060]. The cached tokens are temporarily stored in either “local memory 209” or “memory controller/cache 208” in the ODS server 108. Ex-1003, ¶160; Ex-1006, [0040]; Ex-1010, 157 (“All of these examples of caching share the common attribute that they

increase performance by providing faster access to data, anticipating its potential need in advance, then *storing that data temporarily* where it is rapidly available.”).

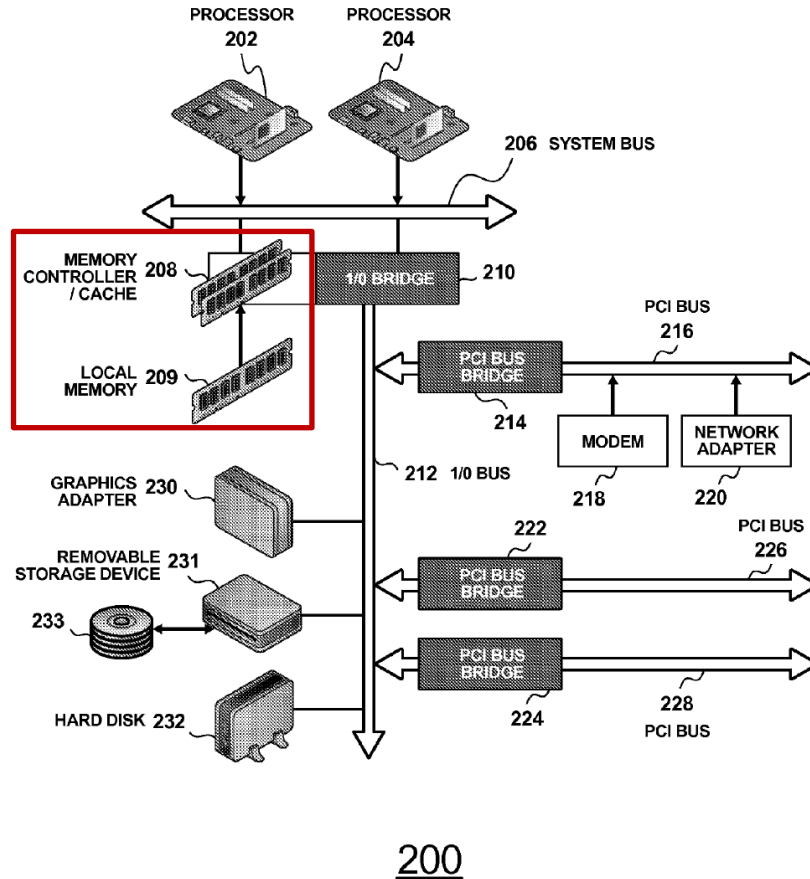


FIG. 2

Id., Fig. 2 (annotated).

In addition, a POSITA would understand that in FIG. 6, when the user ID 602 and password 604 are submitted via page 600, they are stored temporarily in memory at the ODS server 108 in order to communicate them to the financial institution over the Internet 112. Ex-1003, ¶161; Ex-1006, [0069] (“After hitting a ‘next,’ or other

similar button 606, the information contained in the fields 602 and 604 is submitted to the specified financial institution in step 318.”).

eMerchant Demo

Your Purchase

Pay To: eMerchant Demo
 Amount: \$ 1.25 USD

Sign in to your Bank ABC online banking to approve your purchase.

User ID:
 Password:

Next

602
604
606

[Choose a different bank](#)

[Return to Merchant](#)
[Have Questions?](#)

600

FIG. 6

Id., Fig. 6.

163. In an embodiment, Emerson further discloses that “the ODS agent 114 by default or by a consumer’s instruction, does not store the consumer’s log in information.” *Id.*, [0065]. Emerson also discloses that the ODS server 108 contains local memory 209. *Id.*, [0040] (“Referring to FIG. 2, a block diagram of a data processing system that may be implemented as a server, such as server 104, 106, or

108 Also, connected to system bus 206 is memory controller/cache 208, which provides an interface to local memory 209.”). A POSITA would understand that the local memory 209 can be used to temporarily store the account holder’s credentials.

Additionally, Hsu discloses temporarily storing the account holder’s credentials in memory. *See supra* Ground 1, Claim 6, Element [6c]. It would have been obvious to a POSITA to use Hsu’s temporary storage technique in the Emerson system, because Emerson discloses that the ODS agent 114 “does not store the consumer’s log in information” so that “the consumer does not have to worry about his/her private information being obtained by a third party,” Ex-1006, [0065], and Emerson would be able to achieve that by temporarily storing the information for authentication and deleting it afterwards. Ex-1003, ¶163. A POSITA would have a reasonable expectation of success in doing so, because Emerson discloses a similar technique where a type of authentication credentials (*e.g.*, token) is cached (*i.e.*, temporarily stored) for authentication. Ex-1003, ¶163; Ex-1006, [0060].

(5) [6d]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1d]; Ex-1003, ¶164.

(6) [6e]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1e]; Ex-1003, ¶165.

(7) [6f]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1f]; Ex-1003, ¶166.

(8) [6g]

The Emerson/Hsu combination teaches this element. *See supra* Claim 1, Element [1g]; Ex-1003, ¶167.

e) Claim 9

The Emerson/Hsu combination renders claim 6 obvious. *See supra* Claim 4; Ex-1003, ¶168.

f) Claim 10

The Emerson/Hsu combination renders claim 10 obvious. *See supra* Claim 5; Ex-1003, ¶169.

D. Grounds 4, 5, and 6: Obviousness Over Hsu, Hazlehurst, or Emerson/Hsu in view of Peotta (Claims 2, 3, 7, and 8)

1. Summary of Peotta

Peotta relates to the “classification of attacks and vulnerabilities” affecting Internet banking systems. Ex-1007, 1. In particular, Peotta describes a “Short Message Service (SMS)” security method, which “has been applied in some banking systems to notify users about transactions requiring their authorization.” *Id.*, 4. Peotta explains that the SMS method “provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters

which have to informed [*sic*]³ in order to authorize and process the transaction through the online banking system.” *Id.*

Peotta indicates that a vulnerability of the “Short Message Service” security method used in Internet banking systems is that “[t]he attacker may alter the cellular phone number to which the authorization methods are sent.” *Id.*, 5. When the cellular phone number has been altered, a third-party system (here an “attacker”) will be able to provide the authentication needed to access a user’s account without the user’s participation, because the authentication requests would then be sent to a different cellular phone number controlled by the third-party system so that the third-party system may then provide the authentication response needed. *Id.* Thus, Peotta teaches a POSITA a method of authentication on behalf of a user without the user’s participation by rerouting authentication requests to a different phone number. Whereas Peotta describes this system being used by an attacker, that same concept may be used by the user’s agent, such as an authorized third-party system, to enable authentication without the user’s required participation.

³ The authors meant it to read “which have to [*be submitted*] in order to authorize,” based on a similar use of the term “informed” on page 192 of Peotta, where the authors actually meant “submitted”: “When the legitimate user accesses the service, the authentication data *informed* by him is captured by the malware or counterfeit web page which the attacker controls.” Ex-1007, 7.

2. Motivation to Combine Hsu, Hazlehurst, or Emerson/Hsu with Peotta

It would have been obvious to a POSITA to utilize Peotta's teaching of "alter[ing] the cellular phone number to which the authorization messages are sent" in Hsu or Hazlehurst or Emerson/Hsu's systems to provide the benefit of fully automated authentication for systems that are protected by the SMS security method. Ex-1003, ¶¶179–84.

Hsu, Hazlehurst, Emerson/Hsu, and the supposed "attacker" in Peotta share the same goal of accessing a user's online account without requiring a response by the user to any subsequent MFA requests. Ex-1004, [0038]; Ex-1005, 1:41–45; Ex-1006, [0011]. Although Peotta describes "alter[ing] the cellular phone number to which the authorization messages are sent" as a "vulnerability" that may be exploited by an "attacker," it would have been obvious to a POSITA that the technique is equally applicable to benevolent automated authentication that has been consented to by the user, such as in the case of Hsu, Hazlehurst, and Emerson/Hsu. Ex-1003, ¶180; Ex-1007, 5.

Indeed, Hsu, Hazlehurst, and Emerson/Hsu all recognize that MFA presents challenges for automated financial services. Ex-1003, ¶181. Hsu recognizes that "existing financial software is not configured to perform multi-factor authentication in different environments," and that it is therefore "difficult for such financial

software to assemble and share financial information.” Ex-1004, [0005]. Hazlehurst recognizes that existing software “cannot complete automated proxy logins if CAPTCHA [or time-sensitive tokens] is required to gain access or to perform a transaction,” and these security measures thus “present a challenge” for automated services. Ex-1005, 2:21–29. Emerson also notes that “[m]ulti-factor authentication is a relatively-new procedure for ensuring the person accessing the account has permission to do so,” and that “[m]ost banks nowadays require multi-factor authentication when an unusual usage pattern is detected (for example when a user logs in from a new device for the first time).” Ex-1006, [0059], [0070].

In response, Hsu, Hazlehurst, and Emerson/Hsu present solutions allowing automatic access to user’s account to reduce the burden associated with the security requirements. Ex-1003, ¶182. Specifically, Hsu’s “approach to multi-factor authentication allows the financial program to assemble (i.e., retrieve) information for the user in a semi-automated or fully automated fashion,” which “may reduce the burden associated with the security requirements for different documents, host, and/or systems.” Ex-1004, [0038]. Hazlehurst discloses that “automatic logins are accomplished for a subscriber at Internet destinations by use of pre-stored configuration information and user authentication credentials.” Ex-1005, 1:41–45. Emerson’s ODS agent “automatically performs substantially all steps for electronic

communication with a financial institution to gain access to an account.” Ex-1006, [0011]. Adding Peotta’s technique to Hsu, Hazlehurst, or Emerson/Hsu would have provided the known benefit of fully automated authentication for sites that utilize SMS authentication without requiring the user’s participation in the authentication process. Ex-1003, ¶182.

A POSITA would have had a reasonable expectation of success in incorporating Peotta’s SMS authentication technique in the Hsu, Hazlehurst, and Emerson/Hsu systems, in the same manner taught as Peotta, because SMS security is an additional type of “multi-factor authentication” that is like those described in Hsu, Hazlehurst, and Emerson/Hsu. Ex-1003, ¶183. For example, Hsu notes that “multi-factor authentication provided by the user may include ... *telephone numbers*, ... and/or additional personal information.” Ex-1004, [0029]. Hazlehurst notes that “two-factor authentication generally comprises ... Something a person has, such as a *mobile phone*, a credit card or a hardware security token.” Ex-1005, 2:30–36.

The incorporation of “alter[ing] the cellular phone number to which the authorization messages are sent” to automatically perform the SMS security authentication would have been nothing more than the use of a known technique (Peotta’s SMS authentication technique) to improve similar devices (Hsu’s financial program, Hazlehurst’s Pin Vault software, and Emerson/Hus’s ODS agent) in the

same way to yield predictable results (fully automated authentication for accounts protected by SMS security). Ex-1003, ¶184. Although Peotta describes changing the phone number for SMS authentication as a vulnerability when done by an unauthorized third-party, it provides greater flexibility for the user when conducted by an authorized third-party because the user then does not need to provide a response to enable the authorized access to its account information. *Id.* Thus, applying this method to automate account access, as described in the Challenged Claims, would have been a predictable use of existing technology. *KSR Int’l Corp. v. Teleflex, Inc.*, 550 U.S. 398, 417 (2007).

3. Detailed Analysis of Grounds 4, 5, and 6

a) Claim 2

The method of claim 1, further comprising the steps of: storing one or more of the account holder’s endpoints for the online account in a data store associated with the online account; and utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.

The Hsu/Peotta (**Ground 4**), Hazlehurst/Peotta (**Ground 5**), and Emerson/Hsu/Peotta (**Ground 6**) combinations render this element obvious. Ex-1003, ¶¶174–78. Peotta explains that in the SMS authorization method, “banking systems ... notify users,” (*i.e.*, “account holder[s]”) “about transactions requiring

their authorization” by “sending to the user a set of characters” to a “cellular phone number” (*i.e.*, an “endpoint for the online account”). Ex-1007, 4–5. It would have been obvious to a POSITA that Peotta’s statement that an “attacker may alter the cellular phone number to which the authorization messages are sent” would require a “banking system” (*i.e.*, an “online account”) to store the altered phone number in a data store associated with the banking system in order for the system to send “a set of characters” to the altered phone number. Ex-1003, ¶174.

It would have been obvious to a POSITA to incorporate Peotta’s SMS authorization technique with Hsu’s financial program, Hazlehurst’s Pin Vault software, or Emerson/Hsu’s ODS agent (*i.e.*, “the third-party”) to provide the benefit of fully automated retrieval of information from financial accounts protected by SMS authentication (*i.e.*, “without requiring a response by the account holder to any subsequent multi-factor authentication requests”). Ex-1003, ¶175. Hsu’s MFA examples are directed to challenge questions, *e.g.*, “In what city were you born?” or “In what year was your friend born?” Ex-1004, [0035]–[0038]. In Hsu, the challenge question is sent by the server computer 412 to the client computer 410 and a response is returned from the client computer 410 to the server computer 412. *Id.*, [0048]. Hsu discloses that “the financial program ... may retrieve the answer from storage,” enabling information retrieval for the user in a “fully automated fashion” without any need to prompt the user for a response. *Id.*; Ex-1003, ¶175. Hazlehurst’s

examples include time-sensitive tokens. Ex-1005, 1:56–2:6. Hazlehurst discloses that the software “may obtain the correct token file” that is “automatically generated and made available within UPV 113,” and thus “the user need not provide any direct input.” *Id.*, 5:30–37. Emerson also focuses on tokens, and discloses that the ODS agent “may cache (device) tokens set by on-line banking to pass multi-factor authentication,” enabling “a user-free (i.e., user’s further input is not needed) communication session with the financial institution 106.” Ex-1006, [0053], [0060].

Modified to incorporate Peotta’s SMS authorization technique, Hsu’s financial program, Hazlehurst’s Pin Vault software, or Emerson/Hsu’s ODS agent would take the place of the “attacker” described in Peotta. Ex-1003, ¶176. The financial program/Pin Vault software/ODS agent would “alter the cellular phone number to which the authorization messages are sent” to a number accessible by the financial program/Pin Vault software/ODS agent. *Id.* Upon an attempt to retrieve information for the user from the bank, the “set of characters” to be submitted to the bank “in order to authorize and process the transaction through the online banking system” (i.e., “gain access to the online account”) would be sent to the altered phone number accessible by the financial program/Pin Vault software/ODS agent (i.e., “utilizing said one or more endpoints to permit the third-party to gain access to the online account”) instead of the user or the user’s device. *Id.*; Ex-1007, 4.

Like Hsu’s description of “retriev[ing] the answer” to a challenge question “from storage” to avoid prompting the user, the financial program would submit the set of characters (received at the altered phone number) to the bank to provide a “fully automated” retrieval of information. Ex-1003, ¶177; Ex-1004, [0035]-[0038]. Similarly, after obtaining the set of characters, Hazlehurst’s Pin Vault Software would submit it to the bank directly so that “the user need not provide any direct input.” Ex-1003, ¶177; Ex-1005, 5:35. Emerson/Hsu’s ODS agent would do the same to achieve a “user-free” communication session with the bank. Ex-1003, ¶177; Ex-1006, [0053].

Therefore, instead of using an account holder-provided endpoint (e.g., phone number) associated with the user/account holder’s account and “prompting the account holder for a response and receiving a response thereto” as claim 1 recites, the Hsu/Peotta, Hazlehurst/Peotta, and Emerson/Hsu/Peotta combinations each teach using an endpoint (*e.g.*, phone number) “to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests” as claim 2 recites. Ex-1003, ¶178. Accordingly, the Hsu/Peotta, Hazlehurst/Peotta, and Emerson/Hsu/Peotta combinations teach claim 2. *Id.*

b) Claim 3

The method of claim 2, wherein the endpoint includes an email address or a phone number.

The Hsu/Peotta (**Ground 4**), Hazlehurst/Peotta (**Ground 5**), and Emerson/Hsu/Peotta (**Ground 6**) combinations render claim 3 obvious because Peotta teaches that “the endpoint includes ... a phone number” as recited in claim 2: “The attacker may alter the *cellular phone number* to which the authorization messages are sent.” Ex-1003, ¶185; Ex-1007, 5.

c) Claim 7

The method of claim 6, further comprising the steps of: storing one or more of the account holder's endpoints for the online account in a data store associated with the online account; and utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.

The Hsu/Peotta (**Ground 4**), Hazlehurst/Peotta (**Ground 5**), and Emerson/Hsu/Peotta (**Ground 6**) combinations render claim 7 obvious. *See supra* Claim 2; Ex-1003, ¶186.

d) Claim 8

The method of claim 7 wherein the endpoint includes an email address or a phone number.

The Hsu/Peotta (**Ground 4**), Hazlehurst/Peotta (**Ground 5**), and Emerson/Hsu/Peotta (**Ground 6**) combinations render claim 8 obvious. *See supra* Claim 3; Ex-1003, ¶187.

E. Grounds 7, 8, and 9: Obviousness Over Hsu, Hazlehurst, or Emerson/Hsu in view of 2FA Q&A (Claims 2, 3, 7, and 8)

1. Summary of 2FA Q&A

2FA Q&A relates to the question of whether a bank’s “two-factor authentication” is “vulnerable to attack, without hacking the bank’s software or server, or without access to [the user’s] telephone/SMS communications.” Ex-1009, 1. The questioner explains that “[w]hen [the user] attempts to log in to [their] bank, an SMS code is sent to [the user’s] phone,” and the user “then type[s] this nine-character code into the bank’s Web site, to login to [the user’s] account.” *Id.* The questioner indicates that “the only way [they] can imagine” exploitation of the two-factor authentication “would be for someone to install an app on my phone which intercepts SMS traffic and resends the code to an attacker.” *Id.*

In response, the top answer explains that, in addition to intercepting the code, an attacker could “[s]ocial engineer [the user’s] bank to change [the user’s] mobile phone details to a phone [the attacker] control[s],” for example, by “call[ing] [the

user’s] bank pretending to be [the user] and get [the bank] to change the mobile number.” *Id.* As with Peotta above, 2FA Q&A teaches a method of enabling authentication without requiring the user’s participation by rerouting the phone number and having the system at the new phone number provide any required authentication information. *Id.* Whereas 2FA Q&A describes this system being used by an attacker, that same concept may be used by the user’s agent, such as an authorized third-party system, to enable authentication without the user’s required participation.

2. Motivation to Combine Hsu, Hazlehurst, or Emerson/Hsu with 2FA Q&A

It would have been obvious to a POSITA to utilize 2FA Q&A’s teaching of having the user’s bank “change [the user’s] mobile phone details” in Hsu’s financial program, Hazlehurst’s Pin Vault software, or Emerson/Hsu’s ODS agent (*i.e.*, “the third-party”) to provide the benefit of fully automated authentication for systems that are protected by the SMS-based two-factor authentication. Ex-1003, ¶¶198–201.

Hsu, Hazlehurst, Emerson, and the supposed “attacker” in 2FA Q&A share the same goal of accessing a user’s online account without requiring a response by the user to any subsequent MFA requests. Ex-1003, ¶199; Ex-1004, [0038]; Ex-1005, 1:41–45; Ex-1006, [0011]. Although 2FA Q&A describes “[s]ocial engineer[ing] [the user’s] bank to change [the user’s] mobile phone details to a phone

[the attacker] control[s]” as a potential security exploit, it would have nevertheless been obvious to a POSITA that the technique is equally applicable to benevolent automated authentication that has been consented to by the user, such as in the case of Hsu, Hazlehurst, and Emerson/Hsu. Ex-1003, ¶199; Ex-1007, 5. Indeed, as explained above with respect to Grounds 4, 5, and 6, Hsu, Hazlehurst, and Emerson/Hsu all recognize that MFA presents challenges for automated financial services, Ex-1004, [0005]; Ex-1005, 2:21–29; Ex-1006, [0059], [0070], and each present solutions allowing automatic access to user’s account to reduce the burden associated with the security requirements. Ex-1004, [0038]; Ex-1005, 1:41–45; Ex-1006, [0011]. Adding 2FA Q&A’s technique to Hsu, Hazlehurst, or Emerson/Hsu would have provided the known benefit of fully automated authentication for sites that utilize SMS authentication. Ex-1003, ¶199.

A POSITA would have had a reasonable expectation of success in incorporating 2FA Q&A’s SMS-based two-factor authentication technique in the Hsu, Hazlehurst, and Emerson/Hsu systems, in the same manner taught as 2FA Q&A, because SMS-based two-factor authentication is an additional type of “multi-factor authentication” that is like those described in Hsu, Hazlehurst, and Emerson/Hsu. Ex-1003, ¶200; Ex-1004, [0029] (“multi-factor authentication” includes “*telephone numbers*,” “addresses,” and “additional personal information”);

Ex-1005, 2:30–36 (“two-factor authentication generally comprises ... Something a person has, such as a *mobile phone*”); Ex-1006, [0059].

The incorporation of “chang[ing] [the user’s] mobile phone details to a phone” controlled by a third-party in order to automatically perform the SMS two-factor authentication would have been nothing more than the use of a known technique (2FA Q&A’s SMS-based two-factor authentication technique) to improve similar devices (Hsu’s financial program, Hazlehurst’s Pin Vault software, and Emerson/Hus’s ODS agent) in the same way to yield predictable results (fully automated authentication for accounts protected by SMS two-factor authentication). Ex-1003, ¶201. Although 2FA Q&A describes changing the phone number for SMS authentication as a security exploit, when done by an unauthorized third-party, it provides greater flexibility for the user when conducted by an authorized third-party because the user then does not need to provide a response to enable the authorized access to its account information. *Id.* Thus, applying this method to automate account access, as described in the Challenged Claims, would have been a predictable use of existing technology. *KSR*, 550 U.S. at 417.

3. Detailed Analysis of Grounds 7, 8, and 9

a) Claim 2

The Hsu/2FA Q&A (**Ground 7**), Hazlehurst/2FA Q&A (**Ground 8**), and Emerson/Hsu/2FA Q&A (**Ground 9**) combinations render this element obvious.

Ex-1003, ¶¶193–97. 2FA Q&A explains that in a bank’s SMS-based two-factor authentication, when a user (*i.e.*, an “account holder”) “attempt[s] to log in to [the user’s] bank, an SMS code is sent to [the user’s] phone,” (*i.e.*, an “endpoint for the online account”). Ex-1009, 1. It would have been obvious to a POSITA that the top answer’s statement in 2FA Q&A that an “attacker could also ... [s]ocial engineer your bank to change your mobile phone details to a phone [the attacker] controls” would require the bank (*i.e.*, an “online account”) to store the altered phone number in a data store associated with the banking system in order for the system to send “an SMS code” to the altered mobile phone number. Ex-1003, ¶193; Ex-1009, 1.

It would have been obvious to a POSITA to incorporate 2FA Q&A’s SMS-based two-factor authentication technique with Hsu’s financial program, Hazlehurst’s Pin Vault software, or Emerson/Hsu’s ODS agent (*i.e.*, “the third-party”) to provide the benefit of fully automated retrieval of information from financial accounts protected by SMS authentication (*i.e.*, “without requiring a response by the account holder to any subsequent multi-factor authentication requests”). Ex-1003, ¶194. As discussed above with respect to Grounds 4, 5, and 6, Hsu, Hazlehurst, and Emerson/Hsu present various solutions enabling automated authentication without any user input. Ex-1004, [0035]–[0038] (“retrieve the answer from storage”); Ex-1005, 5:30–37 (“obtain the correct token file” from UPV 113);

Ex-1006, [0053], [0060] (“cache (device) tokens set by on-line banking to pass multi-factor authentication”).

Modified to incorporate 2FA Q&A’s SMS-based two-factor authentication technique, Hsu’s financial program, Hazlehurst’s Pin Vault software, or Emerson/Hsu’s ODS agent would take the place of the “attacker” described in the top answer. Ex-1003, ¶195; Ex-1009, 1. The financial program/Pin Vault software/ODS agent would have the bank “change [the account holder’s] mobile phone details to a phone [the financial program/Pin Vault software/ODS agent] control[s].” Ex-1003, ¶195; Ex-1009, 1. Upon an attempt to retrieve information for the user from the bank, the “nine-character code” that is typed “into the bank’s Web site, to login to [the account holder’s] account,” (*i.e.*, “gain access to the online account”) would be sent to the changed phone number accessible by the financial program/Pin Vault software/ODS agent (*i.e.*, “utilizing said one or more endpoints to permit the third-party to gain access to the online account”) instead of the user. Ex-1003, ¶195; Ex-1009, 1.

Like Hsu’s description of “retriev[ing] the answer” to a challenge question “from storage” to avoid prompting the user, the financial program would then submit the SMS code (received at the changed phone number) to the bank to provide a “fully automated” retrieval of information. Ex-1003, ¶196; Ex-1004, [0035]-[0038]. Similarly, after obtaining the set of characters, Hazlehurst’s Pin Vault Software

would submit it to the bank directly so that “the user need not provide any direct input.” Ex-1003, ¶196; Ex-1005, 5:35. Emerson/Hsu’s ODS agent would do the same to achieve a “user-free” communication session with the bank. Ex-1003, ¶196; Ex-1006, [0053].

Therefore, instead of “prompting the account holder for a response and receiving a response thereto” as claim 1 recites, the Hsu/Peotta, Hazlehurst/Peotta, and Emerson/Hsu/Peotta combinations each teach using an endpoint (*e.g.*, phone number) “to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests” as claim 2 recites. Ex-1003, ¶197. Accordingly, the Hsu/Peotta, Hazlehurst/Peotta, and Emerson/Hsu/Peotta combinations obviate claim 2. Ex-1003, ¶197.

b) Claim 3

The Hsu/2FA Q&A (**Ground 7**), Hazlehurst/2FA Q&A (**Ground 8**), and Emerson/Hsu/2FA Q&A (**Ground 9**) combinations render claim 2 obvious because 2FA Q&A teaches that “the endpoint includes ... a phone number” as recited in claim 2: “An attacker could also: ... change your *mobile phone* details to a phone they control.” Ex-1003, ¶202; Ex-1009, 1.

c) Claim 7

The Hsu/2FA Q&A (**Ground 7**), Hazlehurst/2FA Q&A (**Ground 8**), and Emerson/Hsu/2FA Q&A (**Ground 9**) combinations render claim 7 obvious. *See supra* Claim 2; Ex-1003, ¶203.

d) Claim 8

The Hsu/2FA Q&A (**Ground 7**), Hazlehurst/2FA Q&A (**Ground 8**), and Emerson/Hsu/2FA Q&A (**Ground 9**) combinations render claim 8 obvious. *See supra* Claim 3; Ex-1003, ¶204.

V. ENABLEMENT AND SECONDARY CONSIDERATIONS

The prior art references relied upon in this petition are all enabled. Ex-1003, ¶205. There are also no secondary considerations of non-obviousness tied to the Challenged Claims. Ex-1003, ¶206.

VI. CONCLUSION

Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable. Petitioner therefore respectfully requests that IPR be instituted.

DATED: January 15, 2025

Respectfully Submitted,

/Brian M. Buroker/

Brian M. Buroker (Reg. No. 39,125)
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, NW
Washington, DC 20036
Phone: (202) 955-8500
Fax: (202) 467-0539
Email: bburoker@gibsondunn.com

Attorney for Petitioner Plaid Inc.

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Under the provisions of 37 C.F.R. § 42.24(d), the undersigned attorney hereby certifies that the word count for Sections I–VI of the foregoing Petition for *Inter Partes* Review is 13971, according to the word count tool in Microsoft Word.

DATED: January 15, 2025

By: /Brian M. Buroker/

Brian M. Buroker (Reg. No. 39,125)
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, NW
Washington, DC 20036
Phone: (202) 955-8500
Fax: (202) 467-0539
Email: bburoker@gibsondunn.com

Attorney for Petitioner Plaid Inc.

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), (b) on the Patent Owner of Record in the PTO Assignment Branch, Six Trees Capital LLC, via FedEx a copy of this Petition for *Inter Partes* Review, all exhibits, and a Power of Attorney at the Patent Owner's correspondence address of record for the '090 patent:

27267 - WIGGIN AND DANA LLP
ATTENTION: PATENT DOCKETING
437 MADISON AVENUE, 35TH FLOOR
NEW YORK, NY 10022
UNITED STATES

In addition, the Petition, all exhibits, and a Power of Attorney were served through an electronic mail message with a link to counsel of record for Patent Owner and litigation counsel for Patent Owner Identified in Patent Complaint Secure Authentication Technologies, Inc. at the following address and email addresses and also by FedEx to the address given by Secure Authentication Technologies, Inc.'s counsel to the litigation:

For Patent Owner of Record:

Rikesh P. Patel - rpatel@wiggin.com
Jonathan D. Hall – jhall@wiggin.com
ip@wiggin.com
patent@wiggin.com

For Patent Owner Identified in Patent Complaint:

Jonathan E. Pickhardt
QUINN EMANUEL URQUHART & SULLIVAN, LLP
295 5TH AVENUE, 9TH FLOOR
NEW YORK, NY 10016
UNITED STATES

Stephen Q. Wood - stephenwood@quinnemanuel.com
Todd M. Briggs - toddbriggs@quinnemanuel.com
Jonathan E. Pickhardt - jonpickhardt@quinnemanuel.com
Christopher R. Sabbagh - chrissabbagh@quinnemanuel.com

DATED: January 15, 2025

By: /Brian M. Buroker/

Brian M. Buroker (Reg. No. 39,125)
GIBSON, DUNN & CRUTCHER LLP
1700 M Street, N.W.
Washington, DC 20036
Phone: (202) 955-8500
Fax: (202) 467-0539
Email: bburoker@gibsondunn.com

Attorney for Petitioner Plaid Inc.

APPENDIX: CHALLENGED CLAIM LISTING

No.	Limitation
1pre	A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity,
1a	collecting the account holder's credentials;
1b	encrypting the account holder's credentials using one or more processors;
1c	storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
1d	verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
1e	receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
1f	prompting the account holder for a response and receiving the response thereto from the account holder; and
1g	transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.
2	The method of claim 1, further comprising the steps of: storing one or more of the account holder's endpoints for the online account in a data store associated with the online account; and utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.
3	The method of claim 2, wherein the endpoint includes an email address or a phone number.
4	The method of claim 1, wherein the account holder's credentials are collected via a user interface.

No.	Limitation
5	The method of claim 1, wherein the account holder's credentials are collected from a data store.
6pre	A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:
6a	collecting the account holder's credentials;
6b	encrypting the account holder's credentials using one or more processors;
6c	temporarily storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are held in memory;
6d	verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
6e	receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
6f	prompting the account holder for a response and receiving the response thereto from the account holder; and
6g	transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.
7	The method of claim 6, further comprising the steps of: storing one or more of the account holder's endpoints for the online account in a data store associated with the online account; and utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.
8	The method of claim 7 wherein the endpoint includes an email address or a phone number.

No.	Limitation
9	The method of claim 6, wherein the account holder's credentials are collected via a user interface.
10	The method of claim 6, wherein the account holder's credentials are collected from a data store.