

Filed on behalf of Intuit Inc.

By:

JESSICA L. BENZLER, Reg. No. 73,137

MICHAEL J. SACKSTEDER (*pro hac vice* forthcoming)

GEOFFREY R. MILLER (*pro hac vice* forthcoming)

DANIEL LEDESMA (*pro hac vice* forthcoming)

BLAINE SCHMIDT (*pro hac vice* forthcoming)

FENWICK & WEST LLP

One Front Street, 33rd Floor

San Francisco, CA 94111

Telephone: 415.875-2300

Facsimile: 650.938.5200

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTUIT INC.,

Petitioner,

v.

IQX CORP.,

Patent Owner.

Inter Partes Review No. IPR2026-00017

Patent 11,876,924 B2

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT 11,876,924**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. CERTIFICATION OF GROUNDS FOR STANDING	1
III. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED.....	1
IV. OVERVIEW OF THE '924 PATENT	2
A. '924 Patent Specification.....	2
B. Prosecution History	3
C. Priority Date	5
V. LEVEL OF ORDINARY SKILL IN THE ART.....	5
VI. CLAIM CONSTRUCTION	5
VII. GROUNDS FOR INVALIDITY.....	6
A. Ground 1: Claims 1-20 Are Obvious Over Long alone or in View of Gaddis and the General Knowledge of a POSITA	6
1. Long (EX1005)	6
2. Gaddis (EX1006)	10
3. Motivation to Combine Long and Gaddis	12
4. Independent Claim 1	16
a. Long discloses 1[pre].....	16
b. Long discloses 1[a].....	17
c. Long alone or in view of Gaddis discloses 1[b].....	24
d. Long discloses 1[c].....	32
e. Long discloses 1[d].....	34
f. Long discloses 1[e].....	36

TABLE OF CONTENTS
(Continued)

	Page
5. Independent Claim 8	36
a. Long discloses 8[pre].....	36
b. Long discloses 8[a]	36
c. Long discloses 8[b].....	36
d. Long discloses 8[c]	37
e. Long in view of Gaddis discloses 8[d]	37
f. Long discloses 8[e]	37
g. Long discloses 8[f]	37
h. Long discloses 8[g].....	37
6. Independent Claim 15	37
a. Long discloses 15[pre].....	37
b. Long and Gaddis render 15[b] obvious	38
c. Long discloses 15[a], 15[c], 15[d], and 15[e]	39
7. Dependent Claims 2-7, 9-14, and 16-20	39
a. Long discloses claims 2 and 9	39
b. Long discloses claims 3, 10, and 16	41
c. Long discloses claims 4, 11, and 17	41
d. Long in view of Gaddis discloses claims 5, 12, and 18.....	42
e. Long in view of Gaddis discloses claims 6, 13, and 19 obvious.....	43
f. Long discloses claims 7, 14, and 20	45
B. Ground 2: Claims 1-20 Are Obvious Over Louie alone or in View of Gaddis and the General Knowledge of a POSITA	46

TABLE OF CONTENTS
(Continued)

		Page
1.	Louie (EX1007)	46
2.	Gaddis (EX1006)	48
3.	Motivation to Combine Louie and Gaddis	48
4.	Independent Claim 1	51
a.	Louie discloses 1[pre]	51
b.	Louie alone or in view of Gaddis discloses 1[a]	52
c.	Louie alone or in view of Gaddis discloses 1[b]	57
d.	Louie discloses 1[c]	61
e.	Louie discloses 1[d]	62
f.	Louie discloses 1[e]	63
5.	Independent Claims 8 and 15	63
6.	Dependent Claims	67
a.	Louie discloses claims 2 and 9	67
b.	Louie discloses claims 3, 10 and 16	68
c.	Louie discloses claims 4, 11, and 17	69
d.	Louie alone or in view of Gaddis discloses claims 5, 12, and 18	70
e.	Louie in view of Gaddis discloses claims 6, 13, and 19	71
f.	Louie discloses claims 7, 14, and 20	73
VIII.	MANDATORY NOTICES	74
A.	Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))	74
B.	Related Matters (37 C.F.R. § 42.8(b)(2))	74

TABLE OF CONTENTS
(Continued)

	Page
C. Designation of Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3)) and Service of Information (37 C.F.R. § 42.8(b)(4))	75
D. Fees for <i>Inter Partes</i> Review (37 C.F.R. § 42.15(a)).....	75

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	14, 16, 45
STATUTES AND RULES	
35 U.S.C. § 102	<i>passim</i>
35 U.S.C. § 103	1
35 U.S.C. § 120	6
35 U.S.C. § 282	5
35 U.S.C. § 314	1, 6
35 U.S.C. § 319	1
Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)	23, 25, 27
OTHER AUTHORITIES	
37 C.F.R. § 42.22	1
37 C.F.R. § 42.100	1, 5
37 C.F.R. § 42.104	1

EXHIBIT LIST (37 C.F.R. § 42.63(e))

Exhibit	Description
1001	U.S. Patent No. 11,876,924
1002	File History of U.S. Patent No. 11,876,924
1003	Declaration of Benjamin Bederson, Ph.D.
1004	Curriculum Vitae of Benjamin Bederson, Ph.D.
1005	U.S. Patent No. 11,553,074 B1, titled “Methods and Apparatus for Dynamic Application Deeplinking at a Mobile Electronic Device” to Brian Long et al. (“Long”)
1006	U.S. Patent Application Pub. No. 2012/0310752, titled “System, Method, and Computer Program Product for Data Entry Free Electronic Purchasing” to Gaddis (“Gaddis”)
1007	U.S. Patent No. 10,360,627, titled “Systems and Methods to Provide Account Features via Web Based User Interfaces” to Louie (“Louie”)
1008	B. Levine, “Led by TapCommerce founders, startup Attentive launches SMS/MMS marketing platform,” MarTech, dated February 9, 2018, https://martech.org/led-tapcommerce-founders-startup-attentive-launches-smsmms-marketing-platform/
1009	A. Ha, “TapCommerce’s founders are back with Attentive, a messaging startup that’s raised \$13M,” TechCrunch, dated February 8, 2018, https://techcrunch.com/2018/02/08/attentive-launch/
1010	U.S. Patent No. 11,416,829 to Killoran, Jr. et al.
1011	U.S. Patent App. Pub. No. 2007/0150588 to Ghadially et al.
1012	Shopify Help Center, “Abandoned checkouts” (Internet Archive capture dated August 26, 2019)
1013	U.S. Application No. 15/986,569 to Brian Long et al.

Exhibit	Description
1014	Yotpo Support, “Setting User Actions with Yotpo SMS & Email Texts as Rules in Segments” (Internet Archive capture dated April 20, 2024)
1015	Twilio Experience, “Experience Helps Fans Have Live Events With Twilio,” (Internet Archive Capture dated Jan. 23, 2014)
1016	Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(1)(A)(iii)
1017	Fed. Comm’n Commission, FCC 12-21, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 (2012)
1018	Mobile Marketing Association, U.S. Consumer Best Practices for Messaging Version 7.0 (Oct. 16, 2012)
1019	Mobile Marketing Association, Mobile Advertising Guidelines Version 5.0 (2011)
1020	U.S. Patent App. Pub. No. 2014/0024361 to Poon et al.
1021	U.S. Patent App. Pub. No. 2005/0278231 to Teeter
1022	Twilio Ruby Quickstart, “Twilio SMS and MMS Ruby Quickstart” (Internet Archive capture dated Jan. 23, 2014)
1023	U.S. Patent App. Pub. No. 2005/0228899 A1 to Wendkos et al.
1024	Payment Card Industry Security Standards Council, Information Supplement: Best Practices for Securing E-commerce (2017)
1025	U.S. Patent No. 9,298,844 to Graff et al.
1026	U.S. Patent App. Pub. No. 2015/0100483 to Schoenberg
1027	U.S. Patent No. 5,960,411 to Hartman et al.
1028	iReachCompany, “Octane AI Launches Integration for Shopify, Ecommerce Conversational Commerce Platform, and New Partners” (May 1, 2018)

Exhibit	Description
1029	Dan O’Shea, Shopify Adds Facebook Messenger Direct Sales Channel (Oct. 5, 2016)
1030	Gavin O’Malley, Personalized Mobile Messaging: Game-Changer? Q&A With Attentive’s Brian Long (Feb. 7, 2018)
1031	EmailChef, Marketing Glossary, https://emailchef.com/email-marketing-glossary/
1032	Katey Charles Communications, The Ultimate Email Marketing Glossary, https://www.kateycharles.com/glossary#1479408991253-d4e0a31b-8ffd

I. INTRODUCTION

In accordance with 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42.100, Petitioner Intuit Inc. (“Petitioner”) requests *inter partes* review (“IPR”) of claims 1-20 of U.S. Patent No. 11,876,924 to Spindler et al., titled “Secure Transactions Using Customized Webpages” (“’924 patent”; “EX1001”). The ’924 patent is assigned to iQX Corp. (“Patent Owner”) according to USPTO assignment records.

II. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies pursuant to 37 C.F.R. § 42.104(a) that the ’924 patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR challenging the patent claims on the grounds identified in this Petition.

III. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

Pursuant to 37 C.F.R. §§ 42.22(a)(1) and 42.104(b)(1)-(2), Petitioner challenges claims 1-20 of the ’924 patent. This petition, supported by the Declaration of Dr. Benjamin Bederson (EX1003), requests cancellation of claims 1-20 as unpatentable under 35 U.S.C. § 103. *See* 35 U.S.C. § 314(a); EX1003, ¶¶77-302. The grounds include:

Grounds of Unpatentability		
Ground 1	Claims 1-20	35 U.S.C. § 103 over Long in view of Gaddis and the general knowledge of a POSITA
Ground 2	Claims 1-20	35 U.S.C. § 103 over Louie in view of Gaddis and the general knowledge of a POSITA

IV. OVERVIEW OF THE '924 PATENT

The '924 patent claims nothing new. Each of its three independent claims recites the same four steps, and marketers had performed every one of them long before September 27, 2018—the patent's earliest possible priority date. First, the service subscribes a customer to receive messages, such as SMS text messages, after determining that the customer previously provided authentication information like sign-in credentials. Second, the service activates customized web pages and generates secure access information for e-commerce transactions. Third, the service generates a message containing a “customized actionable item”—such as a link to those web pages—keyed to the customer's prior transactions. Fourth, the service sends that message to the customer. Each of those functions was well known in mobile and online marketing and e-commerce long before the '924 patent. EX1003, ¶¶77-110.

A. '924 Patent Specification

The '924 patent specification describes well-known messaging and e-commerce practices. *See* EX1003, ¶¶34-48. It details a standard “opt-in” process. A customer visits “a webpage associated with a client” (i.e., an e-commerce vendor) and “select[s] a box that indicates ‘yes’ they would like to receive text messages.” EX1001, 11:11-15, 13:25-27, 18:23-24. The service then checks whether the customer previously provided a telephone number for such messages. *Id.*, 11:16-18. If so, it may “send a text message to the given subscriber customer with a link to the

customized document showing events of interest.” *Id.*, 11:19-22. That customized document can be a vendor “webpage.” *Id.*, 18:23-24. An “actionable item” (e.g., the link) may then let the customer “purchase tickets or view a customized webpage.” *Id.*, 12:60-61.

The specification describes activating the “customized webpage” in similarly functional terms. The messaging service may “dynamically generate a customized second document 322 (such as a customized second webpage) that includes information about one or more transactions of interest to the individual or subscriber customer.” *Id.*, 9:53-57. The “customized webpage may be curated for the given subscriber customer ... [and] may be updated based on user habits, history, preferences, information from third-party application programming interfaces (APIs) etc.” *Id.*, 10:54-59.

Standard text-messaging technology delivers the message containing the link. The service sends messages to a telephone number by “SMS” or “text message.” *Id.*, 5:27-31. The devices then communicate over the Internet and a cellular telephone network through a base station, or over a wireless local area network through an access point. *Id.*, 4:40-52.

B. Prosecution History

The '924 patent issued from U.S. Patent Appl. No. 18/193,163, filed March 30, 2023. EX1002, 301. Applicant filed preliminary amendments on June 13, 2023 and

September 28, 2023. The second added claims 25-31. Independent claim 25 recited a “customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber.” EX1002, 131-138, 142-148, 166-173.

In a non-final Office Action mailed November 9, 2023, the Examiner rejected claims 2-11, 14-15, and 22-23 under 35 U.S.C. § 102 as anticipated by U.S. Patent Application Pub. No. 2017/0295414 to Murray, objected to claim 24, and allowed claims 25-31. EX1002, 183-189. Applicant then withdrew claims 1-24, retained claims 25-31, amended claim 30, and added system claims 32-44, which recite materially the same matter as the method of claims 25-31. EX1002, 230-238.

The Reasons for Allowance identified no single limitation or point of novelty distinguishing the claims over the prior art. EX1002, 245-246. Instead, the Examiner recited nearly all the limitations of independent claims 25, 32, and 39, then concluded that the prior art “either singularly or in combination” failed to teach them. EX1002, 246. The Examiner allowed no dependent claim on the strength of the feature it adds, noting only that the dependent claims were allowed for the same reason as the independent claims. EX1002, 245; EX1003, ¶¶49-59.

C. Priority Date

The '924 patent claims priority through a chain of applications to Provisional Application Ser. No. 62/737,315, filed Sep. 27, 2018. EX1001, Cover. For this IPR only, Petitioner does not dispute the priority date of September 27, 2018.

V. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner submits that a person having ordinary skill in the art at the time of the invention (“POSITA”) would have had at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a comparable discipline, together with approximately two years of professional experience in the design, development, or implementation of web-based or mobile messaging, electronic commerce, or online transaction systems. Additional education could have substituted for professional experience, and significant work experience could have substituted for formal education. EX1003, ¶¶1-33.

VI. CLAIM CONSTRUCTION

Claim terms subject to IPR are construed using the same standard as used in a civil action under 35 U.S.C. § 282(b), including construing claim terms in accordance with their ordinary meaning as understood by “one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b).

For purposes of this Petition, the challenged claims are interpreted according to their plain and ordinary meaning. EX1003, ¶¶60-63.

VII. GROUNDS FOR INVALIDITY

An IPR petition must demonstrate “a reasonable likelihood” that Petitioner would prevail on at least one claim challenged in the petition. 35 U.S.C. § 314(a). This petition exceeds the threshold.

A. Ground 1: Claims 1-20 Are Obvious Over Long alone or in View of Gaddis and the General Knowledge of a POSITA

1. Long (EX1005)

U.S. Patent No. 11,553,074 B1 to Brian Long et al. (“Long”), titled “Methods and Apparatus for Dynamic Application Deeplinking at a Mobile Electronic Device,” issued January 10, 2023 from Appl. No. 17/496,590 (the ’590 application), filed October 7, 2021. EX1005, Cover. Long is a continuation of Appl. No. 15/986,569 (’569 application), which Brian Long filed May 22, 2018. *Id.*, Cover, 1:5-16. Applicant expressly abandoned the ’569 application in favor of a continuing application on October 8, 2021, a day after the applicant filed the ’590 application. EX1013, 623. The two applications were therefore co-pending, and Long is entitled to the ’569 application’s May 22, 2018 filing date under 35 U.S.C. §§ 120 and 102(d)(2). Every Long disclosure this petition cites appears in the ’569 application because they have the same specification, aside from cross-references to related applications. EX1013, 22-61, 80, 93-122; EX1003, ¶¶113-118. Long also names inventors other than those of the ’924 patent. EX1005, Cover; EX1001, Cover.

Long is thus prior art to the '924 patent under § 102(a)(2), and the Examiner never considered it. EX1001, References Cited.

Long is assigned to Attentive Mobile Inc., an incumbent SMS-marketing company. EX1005, Cover; EX1008, 1.

Long describes a “click-to-text” platform that lets users opt in to receive messages from an e-commerce vendor and complete purchases through links to user-specific checkout pages. EX1005, 1:20-25, 2:18-32. Figure 1 shows three components: click-to-text server 100, containing processor 101 and memory 103; client server 130, associated with a “client,” i.e., an entity or vendor selling goods or services via the internet; and user mobile device 150, which can be any mobile electronic device. *Id.*, Fig. 1, 4:13-17, 4:32-37, 5:39-42, 5:48-50. Memory 103 stores message data 107 (e.g., promotional messages associated with clients), user data 108 (e.g., user phone numbers, a device identifier of the user mobile device, user status as a new or existing user), and client data 109 (e.g., user whitelists and blacklists associated with each client). *Id.*, 4:43-54.

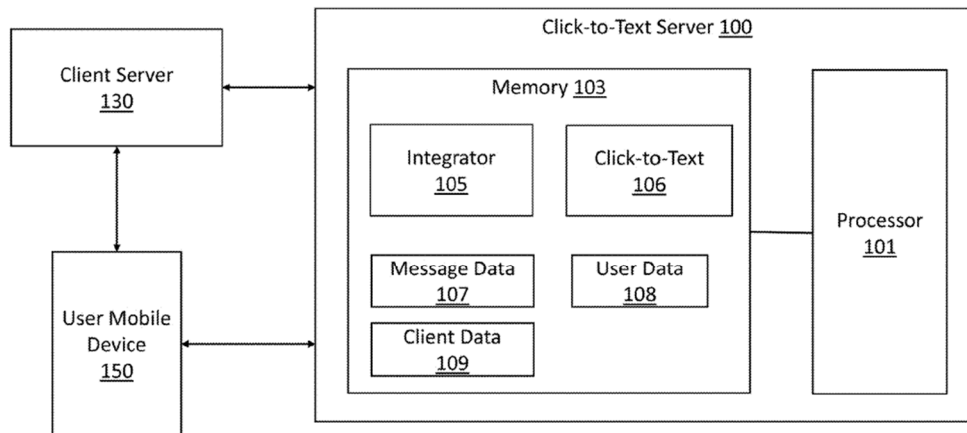


FIG. 1

A user subscribes to messaging-based marketing by selecting a “sign-up” link on the client’s webpage. That link launches the user’s messaging application and pre-populates a text message requesting a subscription, addressed to the client’s telephone number. *Id.*, 3:10-15, 6:58-7:21. The user sends that message to subscribe. *Id.* The click-to-text server then authenticates the user from a user identifier, such as “a user phone number, a sender phone number, [or] a device identifier of the user mobile device,” received through code representing integrator instructions (an “integration tag”) executed on the client’s webpage. *Id.*, 4:59-66, 7:42-56, 11:53-60. The server checks the client’s blacklist or whitelist. *Id.*, 7:57-8:5. “[I]f the user is not on a black list of the client, or if the user is on a white list of the client, the user is authenticated,” after which the server “can provide service and/or send promotional messages.” *Id.*

Long describes a similar mechanism for e-commerce purchases. A customer viewing a shopping cart on a vendor’s website can tap a “1-Step Checkout” link.

Id., 14:52-54, Fig. 5A. The link opens the customer's messaging application with a pre-populated purchase request identifying the shopping cart, the products, and their prices, addressed to the vendor's telephone number. *Id.*, 14:63-15:5, Fig. 5B. When the customer sends it, the click-to-text server authenticates the user from a user identifier, checks the client's black and white lists, and determines whether the user is a new or existing customer. *Id.*, 15:30-41. For a new customer, the server texts a request for shipping and payment information with a "checkout link" that opens a checkout page in a website browser. *Id.*, 15:41-52, Figs. 5C-5D. For an existing customer, the server texts the products in the cart and the shipping and payment information on file, with a "checkout link" where the user can change that information before purchasing. *Id.*, 15:56-16:5, 17:9-24, Figs. 5G-5I.

Long collects and stores data about each customer across transactions. When a customer messages the client's phone number, the click-to-text server "can collect transaction payment data including, but not limited to, the user's payment information (e.g. credit card information, bank account information, or other information), shipping address, and preferred shipping-related settings," and uses that data "to provide a user-friendly purchase experience in subsequent transactions." *Id.*, 12:65-13:7. The server also collects marketing data such as "the type of website content the user has viewed, what items the user has previously purchased, and/or the like." *Id.*, 13:7-14. It stores the customer's "purchase history

associated with the client (e.g., a new/existing customer, previous orders, previous shopping carts, user payment information, user shipping information, and/or the like)” in user data 108 within memory 103. *Id.*, 4:46-51, 16:5-12, 17:25-31. The server draws on that history to identify an existing customer and send the shipping and payment information already on file. *Id.*, 15:56-66.

Long also describes security measures. The click-to-text server generates a unique fingerprint and appends it to each pre-populated message body as a reference, tying the message the customer sends to the click that produced it. *Id.*, 10:54-57. The server can also “append additional data, directly collected or through a third party ... to the user’s phone number as a key value” for “fraud protection or to disable a recently changed number.” *Id.*, 13:14-19; EX1003, ¶¶119-135.

2. Gaddis (EX1006)

U.S. Patent Application Pub. No. 2012/0310752 to Gaddis, titled “System, Method, and Computer Program Product for Data Entry Free Electronic Purchasing,” was filed June 6, 2011, and published December 6, 2012, which predates the September 2018 priority date of the ’924 patent. EX1006, Cover. Gaddis is prior art under at least 35 U.S.C. § 102(a)(1). EX1001, Cover; EX1003, ¶¶136-137. Neither the applicant nor the Examiner cited Gaddis during prosecution of the ’924 patent. EX1001, References Cited.

Gaddis is directed to an e-commerce marketing system in which an “Offer Provider” (either a merchant or “a third party service provider representing multiple merchants”) transmits a promotional message to a user’s “Electronic Communications Account,” including “email, text-SMS, instant messaging-IM, and social networking webpages.” EX1006, ¶¶8, 39. Gaddis embeds in that message a “Promotionally Enabled Link or PEL (e.g., email link, SMS link, or link posted on a User’s social media site ...)” permitting “the User to purchase the services and/or product without entering any alpha numeric data.” *Id.*, ¶8. Each user is “assigned a unique User ID” that “is encrypted,” and the PEL includes “the encrypted User identification (UserId) specific to the User.” *Id.*, ¶¶52-53, 57, 59-60, cls. 5, 19. Anyone other than the intended user who activates the link is diverted to “the merchant’s normal Internet purchase procedure,” not to the user’s accounts. *Id.*, ¶¶10, 59.

The PEL opens “a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User,” displaying the merchant’s logos and “the User’s name,” and the user places the order on that page. EX1006, ¶¶58-59, Figs. 2A-2B, 4B, 10. Because “the User’s shipping and billing information is already on file,” the user checks out without needing to login or enter personal data. *Id.*, ¶¶39, 49; EX1003, ¶¶138-150.

3. Motivation to Combine Long and Gaddis

A POSITA would have been motivated to combine Long’s SMS messaging and checkout architecture with Gaddis’ secure Promotionally Enabled Link (PEL). That combination takes advantage of Long’s integrated e-commerce messaging and customized webpage disclosures while incorporating Gaddis’ security techniques to keep customer information confidential in e-commerce transactions. EX1003, ¶¶151-159.

Long describes a three-entity configuration in which a click-to-text server sends a text message to a customer seeking to complete a purchase on an e-commerce website. EX1005, 15:40-61. The message, which the server sends on behalf of the merchant, includes a custom link to a webpage holding the user’s shopping cart and stored shipping and payment information. *Id.* That link presents a concern with respect to sensitive user information, because the page it opens displays payment and shipping information that Long’s server holds on the customer’s behalf. Long describes the need to secure that information in general terms; Gaddis describes a specific technique. Gaddis builds its secure link from three parameters—a merchant identifier, a deal identifier, and an encrypted User identifier—and encrypts the link before sending it. EX1006, ¶¶34, 57-59. The service provider creates the webpage that link opens using that same information. *Id.* Gaddis delivers that link by text message, defining the PEL as an “email link,

SMS link, or link posted on a User’s social media site,” and stating that a User who selects text confirmation “will receive a text message as demonstrated in Fig. 7 comprising the same PEL.” *Id.*, ¶¶8, 62. Adopting Gaddis’ link would thus not require changing the text-messaging channel Long already uses. EX1003, ¶¶152-153.

Long and Gaddis each support this combination. Long identifies sensitive information as “protected data, proprietary data, personal data, private data,” and discloses mechanisms for protecting it. *See* EX1005, 4:1-11 (defining “data” to include “usernames, passwords,” banking transaction information, and “healthcare information”); *id.*, 7:58-8:5 (authenticating the user against the client’s black and white lists); *id.*, 13:14-19 (appending collected data “to the user’s phone number as a key value” for “fraud protection”). The sensitivity of the data Long’s platform handles was thus a concern, and Long discloses ways to address that risk. Gaddis, for its part, applies encryption techniques “well known in the art” across every deployment it describes. Gaddis states that its invention “may be implemented in a variety of scenarios,” including where “third party service providers may represent various Offer Providers,” and that “[i]n all scenarios, Users are assigned a unique User ID that may be provided to third party service providers” which “is encrypted by methods well known in the art.” *See* EX1006, ¶¶52, 60. A POSITA would thus

recognize that Gaddis’ encrypted identifier operates in the arrangement Long describes. EX1003, ¶¶154-155.

A POSITA combining these teachings would have had a reasonable expectation of success. Long and Gaddis are each analogous art to the ’924 patent. Each is in the same field of endeavor—using links delivered by SMS messaging to give a consumer access to customized webpages for completing online transactions—and each addresses the problem the ’924 patent identifies, that static webpages produce a cumbersome user experience and decrease customers’ willingness and ability to complete e-commerce transactions. EX1001, Title, 1:16-18, 1:29-40, 1:66-2:1, 3:57-4:3; EX1005, 15:41-65, Figs. 5A-5D, 5G-5H. Gaddis’ PEL directs the consumer “to a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User.” EX1006, ¶¶8, 58-59. A POSITA seeking to employ Long’s SMS e-commerce transactions would naturally have looked to available solutions such as Gaddis’ for securing sensitive user information. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 420 (2007) (“[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.”); EX1003, ¶¶156-157.

Encrypting the checkout link as Gaddis describes would be a straightforward change. Both references disclose e-commerce purchase processes involving three

entities: a server that handles messaging and transactions, a vendor, and a customer's mobile device. The modification would not require changing Long's messaging channel, client server 130, or user mobile device 150. EX1003, ¶158; EX1005, 4:66-5:3, 7:57-8:5, 13:5-19, 15:56-16:5, 16:40-17:31, Fig. 1; EX1006, ¶17, Fig. 4A. Long's click-to-text server already composes the link that goes into each message and already identifies each customer from a user identifier it holds. EX1005, 15:31-61. Under the combination, the server composes the same message to the same telephone number, but builds the link from the merchant, deal, and encrypted customer parameters Gaddis describes and encrypts it before sending. EX1006, ¶¶58-59, Figs. 2A-2B, 4B, 10. No additional component is required at the client server or the customer's mobile device, no additional message is sent, and no additional information is stored. EX1003, ¶158.

Further, using encryption to secure a link that reaches sensitive information was a well-known technique. Gaddis itself sends "email links or SMS links" that are "encrypted before sending to User and decrypted by" the offer provider. EX1006, ¶34. Other prior art delivered encrypted, token-based links by SMS to address known security problems with text messaging, and payment-card industry standards treated encrypted transmission of cardholder data across public networks as paramount. EX1003, ¶¶94-97, 159 (citing EX1006, EX1010, EX1023, EX 1024). A POSITA would thus have known that any checkout link in a mobile e-commerce

solution would require “secure access information,” such as an encrypted link, and would readily have had the knowledge to implement it. *Id.*

4. Independent Claim 1

a. Long discloses 1[pre]

Long discloses “**a computer-implemented method.**” Long’s “click-to-text process 700” is executed at “a processor at a server such as the processor 101 of the click-to-text server 100” shown in Fig. 1.

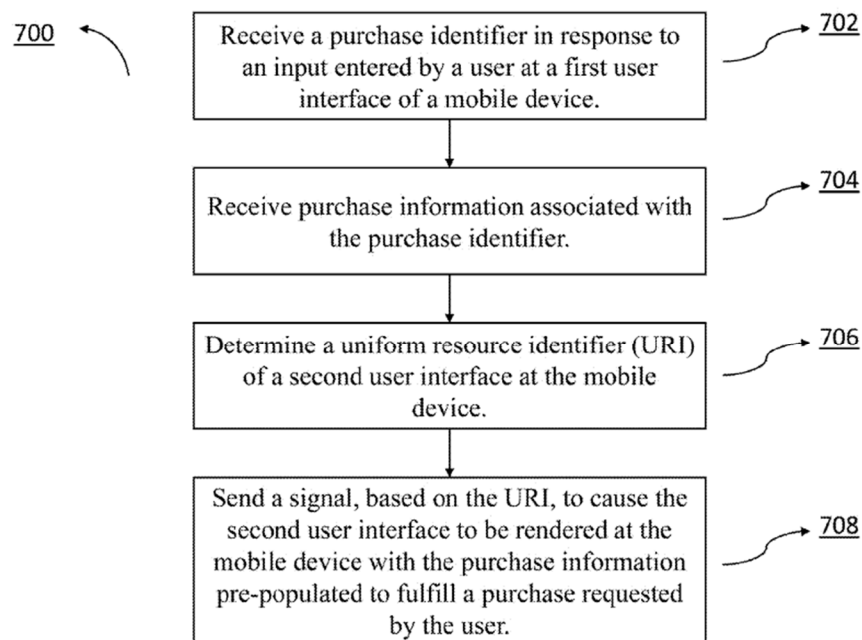


FIG. 7

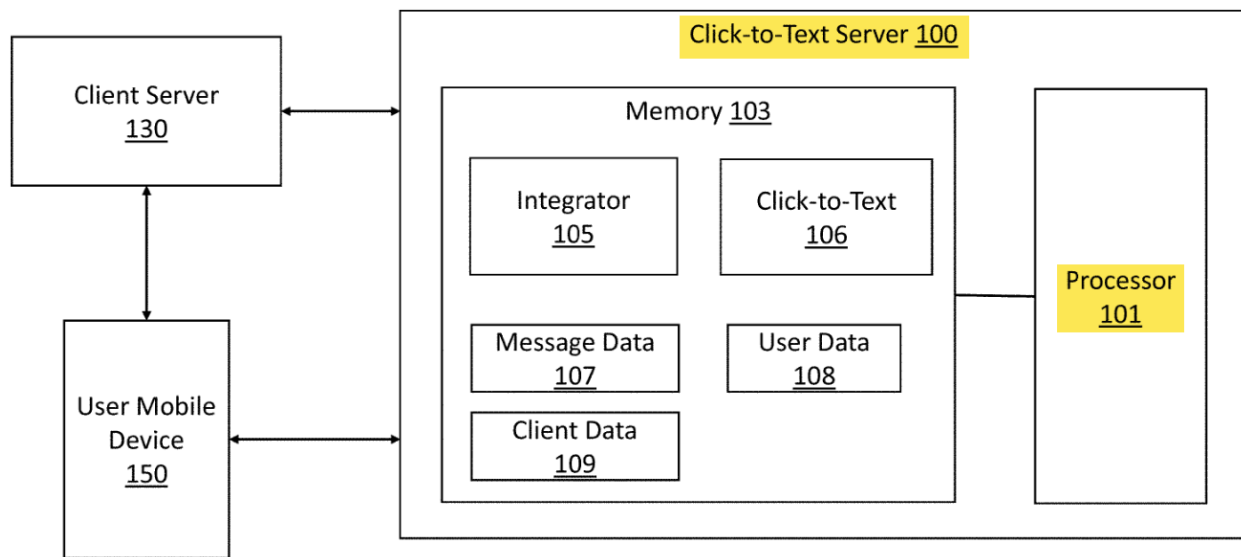


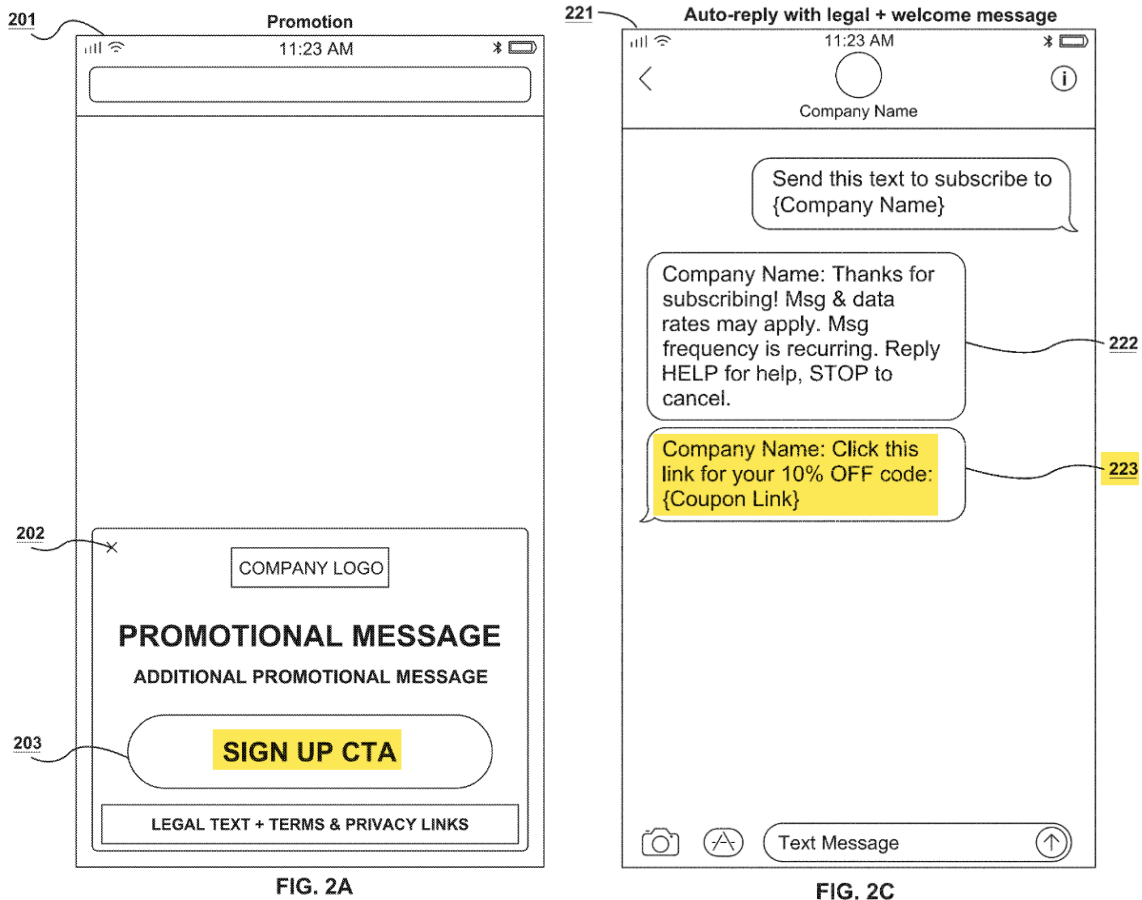
FIG. 1

EX1005, 1:62-64, 2:13-14, 17:32-36, Fig. 7, Fig. 1 (annotated). The click-to-text server can be “a computer” and “include at least one processor 101 and at least one memory 103,” where memory 103 stores “instructions 106 to be executed by the at least one processor 101 to cause the processor to execute the click-to-text process.” *Id.*, 4:32-38; *see also id.*, 4:13-17, 5:3-7. A POSITA would thus have understood that a computer implements Long’s disclosures and the claimed method. EX1003, ¶¶112, 160-161.

b. Long discloses 1[a]

Long discloses “**configuring a service subscriber associated with a telephone number, to be subscribed to receive additional content at the telephone number, in response to determining that the service subscriber has previously provided authentication information.**”

Long discloses the click-to-text server “**configuring a service subscriber associated with a telephone number to be subscribed to receive additional content at the telephone number.**” Long’s click-to-text server stores “a user’s subscription status associated with the client.” EX1005, 8:6-21. The user subscribes to the client (e-commerce vendor) by clicking a “sign-up” link on a website, email, or text message, which opens the user’s messaging application with a pre-populated message that the user sends to the client’s phone number to join a subscription list. *Id.*, 6:48-57, 6:63-7:21, Fig. 2A (annotated). The server confirms the subscription, and the user may thereafter receive marketing information (additional content) from the client. *Id.*, 7:35-41, Figs. 2B-2C (annotated).



The click-to-text server associates the subscriber with a telephone number. The server stores “user data” including “user phone number, user device identifier, other information identifying the user or the user mobile device.” EX1005, 4:46-48. It authenticates the user based on a “user identifier,” which can be “a user phone number, a sender phone number, a device identifier of the user mobile device.” *Id.*, 7:53-56. When the user sends the message to the client’s phone number, the server collects “transaction payment data” such as the user’s credit card, bank account information, and shipping address, along with “marketing-based data” including “user preferences regarding what type of message, or other information” and the

user's "shipping address[]" and preferred shipping-related settings." *Id.*, 12:65-13:14. The server can append that data "to the user's phone number as a key value," which it can then use for fraud protection or to disable a changed number. *Id.*, 13:14-19.

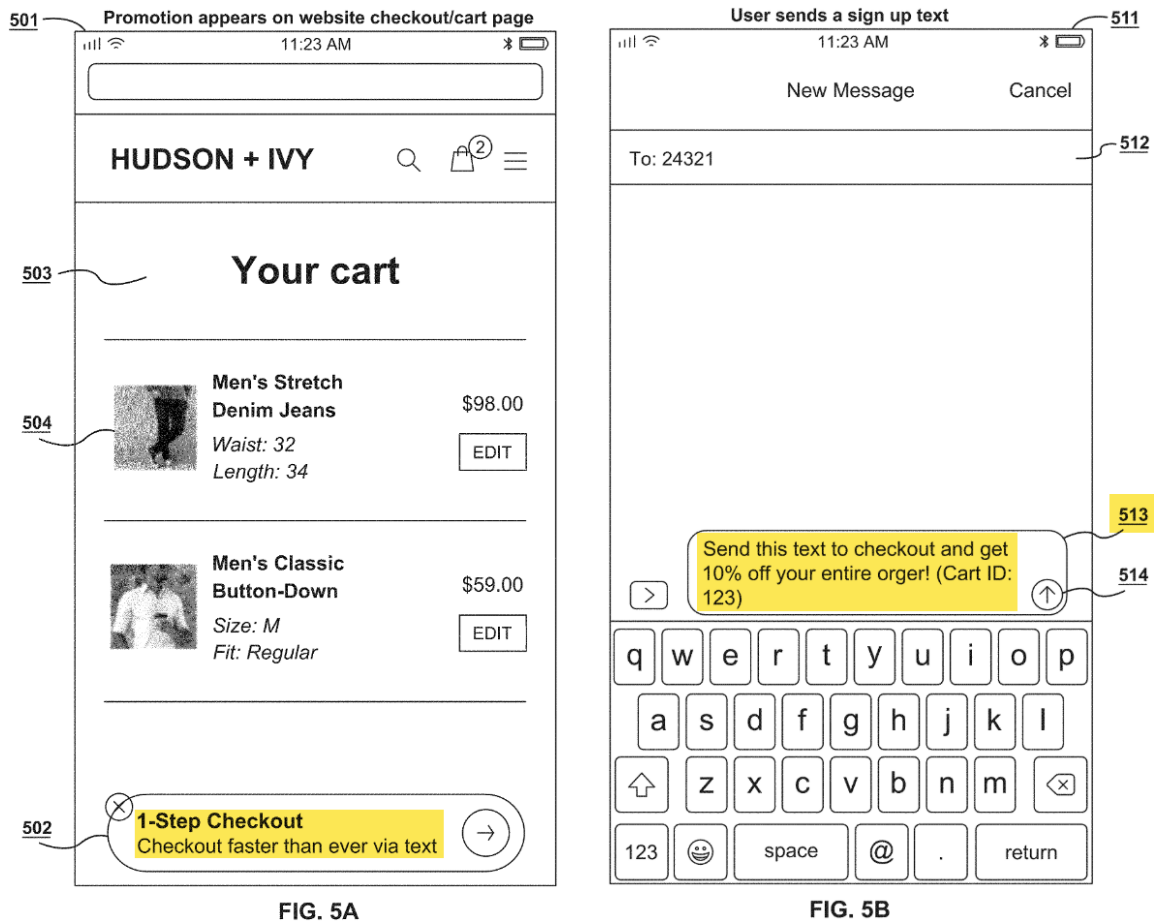
Once the user is subscribed, the click-to-text server "can provide service and/or send promotional messages 223 to the user." *Id.*, 7:62-67; *see also id.*, 3:10-15 ("the user can be subscribed to [the] service to receive messaging based marketing information from the recipient when the message is sent"). By joining the user to the subscription list and associating the user with a telephone number, the server configures the user to be subscribed to receive marketing and purchase information at that number. EX1003, ¶¶162-163.

Long also discloses, in multiple embodiments, configuring a service subscriber to be subscribed to receive additional content at the telephone number **"in response to determining that the service subscriber has previously provided authentication information."**

First, when the user clicks the "sign-up" link, the user device sends an HTTP POST request notifying the server of that selection. EX1005, 8:55-59, Fig. 2A. The request includes "a user identifier (e.g., a user phone number, a user mobile device identifier, user impression data, a user agent field collected by the web browser, and/or any information identifying the user and/or user mobile device)." *Id.*,

8:65-9:1; *see also id.*, 9:12-13. When the user sends the ensuing pre-populated message 213, the server authenticates the subscriber using the identifier the subscriber *already provided* by clicking the link. Long explains that the server “can authenticate the user based on a user identifier”—the same information from the HTTP POST request—and can “receive the user identifier *prior to* receiving the message 213” that subscribes the user to additional marketing information. *Id.*, 7:42-48, Fig. 2B. Long thus discloses configuring the subscriber to receive additional content at the telephone number in response to determining that the subscriber previously provided the user identifier (authentication information) in the HTTP POST request. EX1003, ¶164.

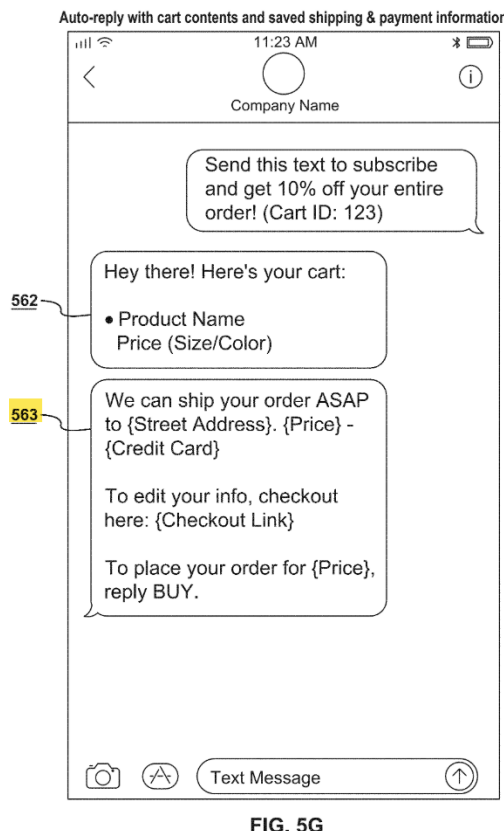
Second, Long discloses an embodiment where the subscriber purchases items in their shopping cart on a client website. EX1005, 14:50-54. The user taps “1-Step Checkout,” and the user’s messaging application will open with a pre-populated purchase message.



EX1005, 14:52-54, 14:63-15:5, Figs. 5A-5B (annotated).

Once the click-to-text server receives the message, it “can authenticate the user based on a user identifier,” and “determine, based on the user identifier, if the user is a new customer of the client or an existing customer of the client.” *Id.*, 15:30-41. For an existing customer, the server sends through the messaging application “message 563 informing the user of the shipping information and the payment information on file associated with the user.” *Id.*, 15:56-66, Fig. 5G (annotated below). Checking whether the user is an existing customer from the user identifier is a determination that the user previously provided authentication

information, which the server makes before configuring the subscriber to receive the checkout link. EX1003, ¶165.



Third, while authenticating the user during the “1-Step Checkout” flow, the click-to-text server also “determine[s] if the user is on a black list or on a white list associated with the client.” EX1005, 15:36-38. A POSITA would understand that a user could be on a “white list associated with the client” by previously providing information permitting such correspondence. Long confirms this, teaching that a user receives messages only after opting in, to ensure “compliance with the Telephone Consumer Protection Act of 1991 (“TCPA”) and the regulations by trade

associations representing the wireless communication industry (e.g., CTIA).” EX1005, 6:53-57; EX1003, ¶166 (citing EX1031-EX1032).

c. Long alone or in view of Gaddis discloses 1[b]

Long in view of Gaddis discloses **“activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction, the activating comprising generation of secure access information for performing the e-commerce transaction.”**

Long discloses **“activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction.”** Long discloses a click-to-text purchase process that a user begins by tapping the “1-Step Checkout” link 502 displayed on first user interface 501 (e.g., a website browser), which initiates second user interface 511 (e.g., a messaging application). EX1005, 14:50-67, Figs. 5A-5B (annotated).

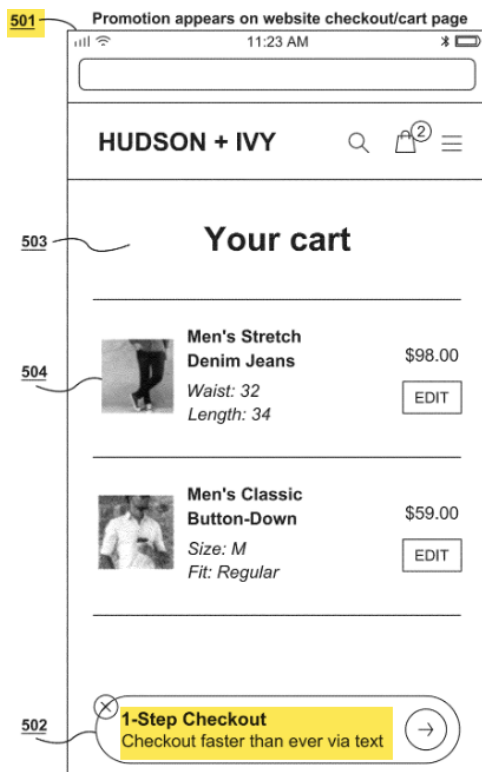


FIG. 5A

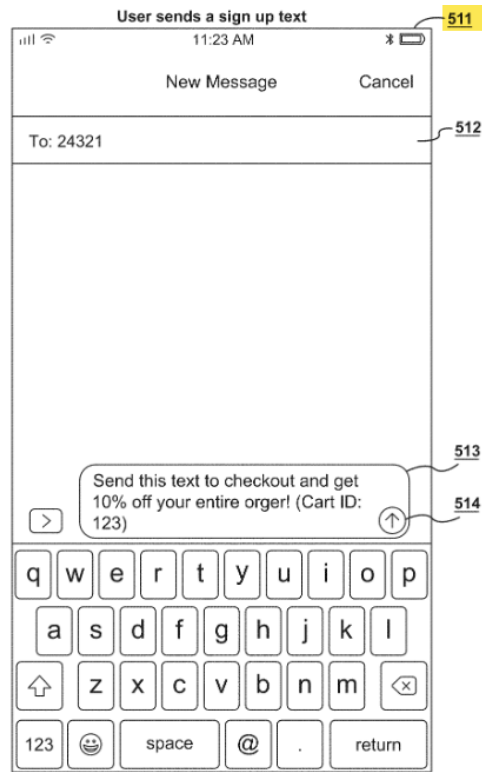


FIG. 5B

The click-to-text server sends the user messages via the messaging application. *Id.*, 15:30-61. What messages the user receives depends on whether the user is a new or existing customer. *Id.* If the user is new, the click-to-text server will send a message 522 requesting shipping and payment information, along with a checkout link to facilitate entry of this information. *Id.*, 15:41-55, Fig. 5C (annotated). If the user is an existing customer, the click-to-text server will send message 562 including shopping cart information and message 563 informing the user of the shipping and payment information on file for the user. *Id.*, 15:56-16:2, Fig. 5G (annotated below).

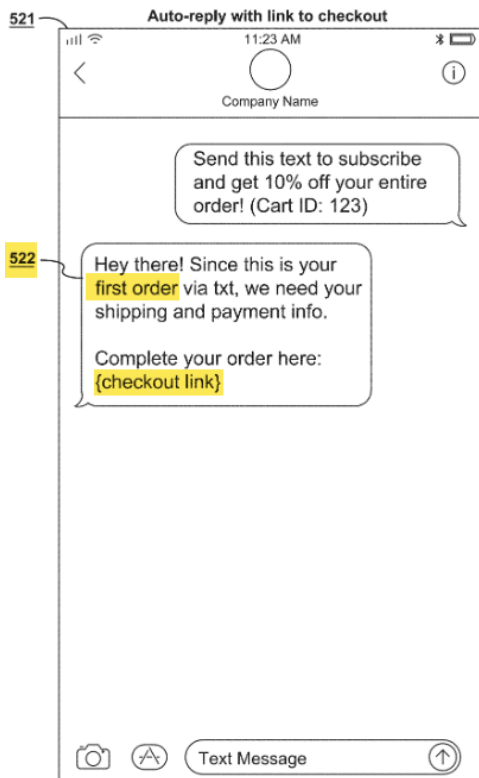


FIG. 5C

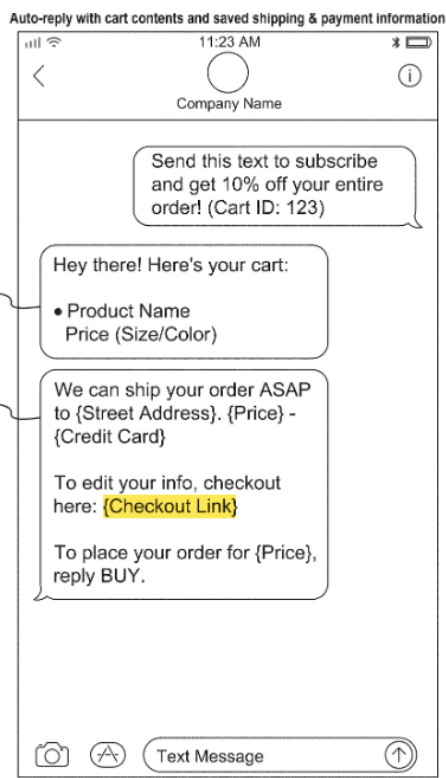


FIG. 5G

Messages 522 and 563 include a “checkout link” that, when clicked, opens a third user interface—the checkout page 531—which can be the same as the first user interface (i.e., the client’s e-commerce website in Fig. 5A), where the user can input shipping and payment information if they are a new customer or change their information if they are an existing customer. EX1005, 15:49-52 (third user interface display), 15:53-55 (message confirming the order has been placed); *see also id.*, 12:65-13:7 (storing user payment information), 17:3-8, Figs. 5C-5G.

FIG. 5D

A POSITA would have recognized that the checkout page is a “customized webpage” because it is specific to the user’s customer status and shopping cart, and, in the case of an existing customer, it includes previously supplied payment and shipping information. EX1003, ¶¶167-169. A POSITA would have considered the checkout link to be a “customized actionable item for performing an e-commerce transaction” and to be “include[d]” with the customized webpage because it is specific to the user’s purchase and links to and opens the checkout page for performing the purchase. *Id.* This understanding is consistent with the ’924 patent disclosure, “The message may include an actionable item, e.g., a link to purchase tickets or view a customized webpage, such that the subscriber customer can send a command ... to view the customized webpage or purchase tickets,” and also the scope of dependent claim 5, which separately recites that “the customized actionable item comprises a secure link.” EX1001, 12:60-61, cl. 5; EX1003, ¶¶169-171.

A POSITA would have also understood that Long discloses “activating one or more customized webpages” because the checkout link in Long’s message opens a webpage that displays that subscriber’s order, and in the case of an existing customer, includes a user’s existing shipping information. EX1003, ¶¶172 (citing EX1005, 15:45-47, Figs. 5C-5D).

Long alone or in view of Gaddis discloses **“the activating comprising generation of secure access information for performing the e-commerce**

transaction.” Long discloses security measures for the e-commerce transactions. The click-to-text server generates a unique fingerprint and appends it as a reference to the body of pre-populated messages, so that the message the customer sends is tied to the particular click that produced it. EX1005, 10:54-57. The server can also “append additional data, directly collected or through a third party ... to the user’s phone number as a key value,” which is used for “fraud protection or to disable a recently changed number.” *Id.*, 12:65-13:19.

A POSITA would have found the “generation of secure access information” limitation obvious in light of Long alone. Long explains that disclosing user information should be avoided, teaches appending collected data to the subscriber’s phone number as a key value used “for fraud protection” and to disable a changed number, *id.*, 13:15-19, and screens each subscriber against the client’s “black list” and “white list” before responding, *id.*, 15:30-38. A POSITA generating a link that reaches stored payment credentials would have secured that link as a matter of routine design. EX1003, ¶¶173-174.

Even if Long did not disclose the “generation of secure access information” limitation, Gaddis does. *Id.*

Gaddis’ “electronic message generation module 408” transmits messages “comprising encrypted links unique to each User,” referred to as Promotionally Enabled Links (PEL), which a POSITA would understand to be “secure access

information.” EX1006, ¶53; EX1003, ¶¶175-176. Gaddis defines the PEL as “a computer programming link generated as part of invention that contains Promotional Information, is encrypted before sending to User and decrypted by OP to facilitate purchase.” *Id.*, ¶¶34-35. The PEL includes three parameters—“?deal=123,” “?merchant=xyz,” and a “custhash=9098788492” that is an “encrypted User identification (UserId) specific to the User”—along with promotional information such as the User ID number, offer, and target URL. *Id.*, ¶¶34-35, 59.

A POSITA would recognize that the PEL is “generated” as part of activating a custom webpage. Gaddis’ service provider generates it when it “generates and transmits an advertisement,” before transmission, *id.*, ¶59, and its “webpage document generation module” creates the webpage the PEL opens, *id.*, ¶53. The service provider uses “[t]he information exchanged” to “create a webpage specific to a merchant comprising the merchant’s identifying information, such as logos or trademarks, and the User’s name,” and “a webpage specific to each User’s requirements.” *Id.*, ¶58. When the User “clicks (click 1) on the PEL,” the User is “re-directed to a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User,” and the encrypted custhash identifies which User that page is for. *Id.*, ¶59; EX1003, ¶177.

A POSITA would recognize that Long could be modified so its SMS checkout link—the customized actionable item—incorporates the security characteristics of

Gaddis' PEL. Long's click-to-text server would generate the checkout link it sends in a message as a PEL built from a merchant identifier, a deal identifier, and an encrypted user identifier, encrypt that link before transmission, and generate the checkout page that link opens using that same information. EX1005, 15:56-66, Fig. 5G; EX1006, ¶¶34, 57-59; EX1003, ¶178.

In the combination, when the subscriber taps the PEL in Long's messaging application, the link "redirects to the service provider"—here, Long's click-to-text server. EX1006, ¶59; EX1005, 11:18-21, 15:56-65. The server decrypts the link, which Gaddis states is "decrypted by OP to facilitate purchase," yielding "?deal=123," "?merchant=xyz," and the "custhash" identifying the User. EX1006, ¶¶34, 59. The server resolves custhash against its user database, which holds "previous orders, previous shopping carts, user payment information, user shipping information." EX1005, 16:5-12. The subscriber is then "re-directed to a webpage hosted by the service provider and created specifically for the merchant's advertisement and the User," customized to that subscriber based on the contents of the link as described in Gaddis. EX1006, ¶¶53, 58, 59; EX1003, ¶179.

For the reasons given in Section VII.A.3, incorporated here, a POSITA would have been motivated to make this combination to achieve the security objectives Long already states, and would have had a reasonable expectation of success. *See, e.g.,* EX1005, 10:54-57, 12:65-13:19 (describing fraud protection and other security

measures). Incorporating Gaddis’ encrypted PEL—which carries a user-specific encrypted identifier that the server decrypts to build the subscriber’s webpage—further that objective, keeping the subscriber’s checkout information secure and available only to that subscriber. EX1006, ¶¶34, 58-59; EX1003, ¶180.

Such a combination puts together prior art elements according to known methods to yield predictable results, as well as use of a known technique to improve a similar method in the same way. Creating encrypted links that include a user-specific identifier to protect user information in e-commerce was well-known at the priority date of the ’924 patent. *Supra* Section VII.A.3; EX1003, ¶¶87-90. A POSITA would thus naturally look to prior art disclosing such encrypted-link mechanisms, such as Gaddis, to incorporate the practice into Long’s similar three-entity architecture for SMS checkouts—i.e., this combination would be obvious to a POSITA, both to implement and to try. EX1003, ¶¶180-181.

A POSITA would have a reasonable expectation of success in making this modification. *Id.*, ¶¶182. Although Gaddis illustrates its flow using email and social media accounts, Gaddis also expressly defines its PEL as an “email link, SMS link, or link posted on a User’s social media site,” delivers it to an account that may be “email, text-SMS, instant messaging-IM, and social networking webpages,” and tracks “which link channel the purchase was made from (e.g., email, SMS, IM, Facebook®, Twitter®).” EX1006, ¶¶8, 39, 59. A User selecting text confirmation

“will receive a text message as demonstrated in Fig. 7 comprising *the same PEL*.” *Id.*, ¶62 (emphasis added). Gaddis even adds that the User “will view the same electronic messages and webpages, and proceed through the same ‘no data entry’ process” across embodiments, and that “[o]ne of ordinary skill in the art would readily know of synonymous system architectures.” *Id.*, ¶¶53, 60.

Finally, limitation 1[c] requires that the “customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber,” which under this combination will include Gaddis’ encryption characteristics. Gaddis’ encryption technique is compatible with that requirement. Its Offer Provider must have the User’s contact, shipping, and billing information on file before sending the advertisement, including billing information “sufficient to complete a financial transaction.” EX1006, ¶8. Gaddis thus teaches that its PEL is used in scenarios, as disclosed in Long, where a checkout link corresponds to prior actions associated with one or more prior transactions performed by the service subscriber. *See infra* Section VII.A.4.d (limitation 1[c]); EX1003, ¶183.

d. Long discloses 1[c]

Long discloses “**wherein the at least one customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber.**”

As discussed in limitation 1[b], Long discloses a “customized actionable item”—a “checkout link” that launches a checkout page (customized webpage) for the customer (service subscriber) when selected.

That link also corresponds to the claimed “prior actions.” Long’s click-to-text server collects the user’s payment information, shipping address, and preferred shipping-related settings during a transaction to provide a user-friendly purchase experience in subsequent transactions. EX1005, 12:65-13:7, Fig. 5G. It also collects marketing data recording “what items the user has previously purchased.” *Id.*, 13:7-14. On a

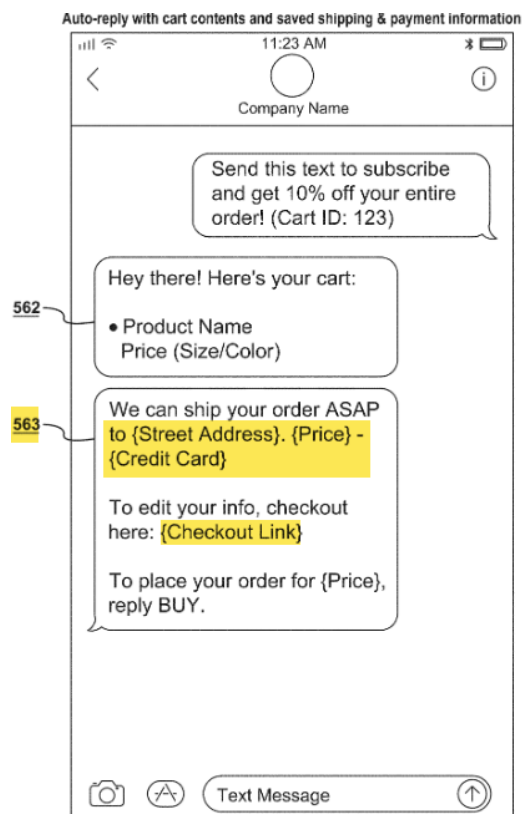


FIG. 5G

subsequent purchase, the server informs an existing customer of the shipping and payment information on file and sends a checkout link opening a page where the user can change it. *Id.*, 15:56-16:12, Figs. 5G-5H.

A POSITA would have recognized that Long’s tailored messages and its link to a checkout page populated from the user’s prior purchases disclose a customized actionable item corresponding to prior actions associated with one or more prior transactions performed by the user. EX1003, ¶¶184-186.

e. Long discloses 1[d]

Long discloses “**generating, for the service subscriber, a third party message associated with the one or more customized webpages, the third party message including the at least one customized actionable item.**”

As noted above, Long discloses a message including the at least one customized actionable item, which in this combination carries Gaddis’ security characteristics. *See supra* Section VII.A.4.c (limitation 1[b]). The click-to-text server generates that message and sends it to the user as message 563, which includes a checkout link for completing a purchase, via second user interface 521, a messaging application. EX1005, 15:41-66.

A POSITA would understand that message 563 is a “third party message” because the server sends it on behalf of the client—an entity, such as an e-commerce vendor—distinct from the user and the click-to-text server. *Id.*, 6:34-36 (describing client as “an entity selling or providing a good(s) or service(s) via the internet”), Fig. 1 (separating client server, user mobile device, and click-to-text server) (annotated).

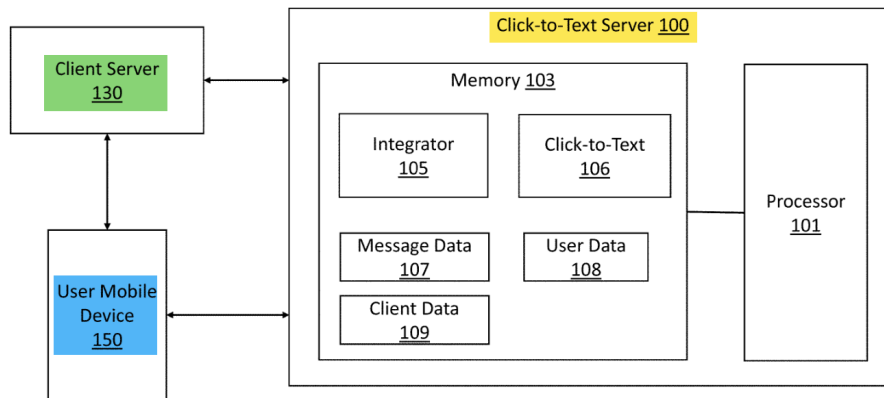


FIG. 1

When clicked, the checkout link in message 563 opens a third user interface showing a checkout page for completing the user’s purchase with the client. EX1005, 15:61-66. The message is therefore associated with the customized webpages because it includes information about the checkout the user seeks to complete, such as shipping and product information, along with a link to the custom checkout webpage. EX1003, ¶¶187-190.

This is also consistent with the Long-Gaddis combination for the encrypted checkout link. Gaddis resolves the encrypted link to redirect the user to a customized webpage. *Supra* Section VII.A.4.c (citing EX1006, ¶¶53, 58, 59). That compatibility supports the reasonable expectation of a successful combination and confirms that the checkout link (customized actionable item) is associated with the customized webpages as claimed. EX1003, ¶191.

A POSITA would thus have understood that the click-to-text server generates for the user (“service subscriber”) a client (“third party”) message associated with

the checkout page (“customized webpage”), and that the message includes the checkout link (“customized actionable item”). EX1003, ¶192.

f. Long discloses 1[e]

Long discloses “**causing transmission of the generated third party message to the service subscriber,**” because the click-to-text server sends (“causes transmission of”) message 563 (the “generated third party message”) to the user (“service subscriber”). *See supra* Section VII.A.4.e; EX1003, ¶193.

5. Independent Claim 8

a. Long discloses 8[pre]

Long discloses “**a system.**” EX1003, ¶194. Long’s click-to-text system includes click-to-text server, client server, and user mobile device. EX1005, 4:32-38.

b. Long discloses 8[a]

Long discloses “**a processor.**” EX1003, ¶195. Long’s click-to-text server includes at least one processor, EX1005, 4:32-38, Fig. 1, and Long discloses that the click-to-text process is executed at processor 101. *Id.*, 17:32-41, Fig. 7.

c. Long discloses 8[b]

Long discloses “**memory configured to store program instructions, wherein, when executed by the processor, the program instructions cause the processor to perform operations.**” EX1003, ¶196. Long’s memory 103 stores click-to-text instructions 106 that are executed by processor 101 to perform click-to-

text process 700 as illustrated in the flow chart in Fig. 7. EX1005, 4:32-38, 5:3-7, 17:32-41, Figs. 1, 7.

d. Long discloses 8[c]

As stated in limitation 1[a], Long discloses limitation 8[c]. *Supra* Section VII.A.4.b; EX1003, ¶197.

e. Long in view of Gaddis discloses 8[d]

As stated in limitation 1[b], Long and Gaddis render limitation 8[d] obvious. *Supra* Section VII.A.4.c; EX1003, ¶198.

f. Long discloses 8[e]

As stated in limitation 1[c], Long discloses limitation 8[e]. *Supra* Section VII.A.4.d; EX1003, ¶199.

g. Long discloses 8[f]

As stated in limitation 1[d], Long discloses limitation 8[f]. *Supra* Section VII.A.4.e; EX1003, ¶200.

h. Long discloses 8[g]

As stated in limitation 1[e], Long discloses limitation 8[g]. *Supra* Section VII.A.4.f; EX1003, ¶201.

6. Independent Claim 15

a. Long discloses 15[pre]

Long discloses “**a non-transitory computer-readable storage medium for use in conjunction with a computer, the computer-readable storage medium**

storing program instructions that, when executed by the computer, cause the computer to carry out one or more operations.” Long’s memory 103 stores click-to-text instructions 106 executed by processor 101. EX1005, 4:32-38, 5:3-7, Fig. 1. Long explains that its implementations relate to a “non-transitory computer-readable medium” having instructions or computer code for performing computer-implemented operations, non-transitory “in the sense that it does not include transitory propagating signals per se (e.g., a propagating electromagnetic wave carrying information on a transmission medium such as space or a cable).” *Id.*, 20:26-52. A POSITA would have understood memory 103 storing instructions 106 to be such a non-transitory medium. EX1003, ¶202.

b. Long and Gaddis render 15[b] obvious

Limitation 15[b] combines limitation 1[b] with the subject matter claim 2 adds to claim 1. Like 1[b], it recites “activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction,” with “the activating comprising generation of secure access information for performing the e-commerce transaction.” It adds that the transaction is “to purchase tickets, merchandise, or products or view the one or more customized webpages depicting information about the tickets, merchandise, or products”—claim 2’s added limitation. EX1001, 20:66-21:3, 22:25-28. Long and Gaddis render each element obvious for the reasons given for limitation 1[b] and for claims 2 and

9. A POSITA would have understood that Long and Gaddis meet 15[b]. Long's checkout link opens a page where the user buys the client's goods, and Gaddis' encryption secures that link. *See supra* Section VII.A.4.c; *infra* Section VII.A.7.a; EX1003, ¶204.

c. Long discloses 15[a], 15[c], 15[d], and 15[e]

Limitations 15[a], 15[c], 15[d], and 15[e] are identical to limitations 1[a], 1[c], 1[d], and 1[e], respectively. For the reasons given above for those limitations, Long discloses each of them. *See supra* Sections VII.A.4.b, VII.A.4.d-f; EX1003, ¶¶203, 205-207.

7. Dependent Claims 2-7, 9-14, and 16-20

Each claim addressed below depends from claim 1, claim 8, or claim 15. As shown above, Long in view of Gaddis discloses every limitation of those independent claims. *See supra* Sections VII.A.4-VII.A.6. The discussion below addresses only the feature each dependent claim adds.

a. Long discloses claims 2 and 9

Long and Gaddis render obvious dependent claims 2 and 9: **“the at least one customized actionable item comprises data to access the one or more customized webpages, the data being configured to enable the service subscriber to purchase tickets, merchandise, or products or view the customized webpages depicting information about the tickets, merchandise, or products.”**

As noted above, the “customized actionable item” in the Long-Gaddis combination is the Promotionally Enabled Link that the click-to-text server builds from a merchant identifier, a deal identifier, and an encrypted user identifier and sends to the subscriber in message 563 as the “checkout link.” EX1005, 15:62-66; EX1006, ¶¶34, 58-59; *see also supra* Section VII.A.4.c. That link is associated with the checkout page that opens when the subscriber taps it, and Gaddis explains that the link redirects the user to that page upon selection. EX1005, 15:45-49, 15:62-66; EX1006, ¶59.

A POSITA would understand that the checkout link “comprises data to access the one or more customized webpages ... the data being configured to enable the service subscriber to purchase ... products” because it lets subscribers reach their checkout pages directly to complete purchases. EX1005, 15:45-52, 15:62-66; EX1006, ¶¶58-59; EX1003, ¶¶208-211.

The page the link opens is a webpage. Long’s third user interface “can be the same as the first user interface 501 (e.g., a website browser).” EX1005, 15:47-49. Long also discloses purchasing products. The first user interface displays “a shopping cart 503 with products 504 to be purchased,” and the purchase request identifies “a product identifier, a product name, a product description, a price of each product.” *Id.*, 14:52-54, 14:67-15:3.

Gaddis discloses that the PEL opens a webpage created for the User and built from the User's information on file, which "describes the product or service, and optionally, the quantity that may be purchased," so that the User proceeds through a "no data entry" checkout process. EX1006, ¶¶48-49, 53, 58-60; EX1003, ¶¶212-213.

b. Long discloses claims 3, 10, and 16

Long discloses **"the third party message is associated with a third party ticket provider, a third party service provider, or a third party event provider."** The messages the click-to-text server sends via the client phone number are associated with the client, an entity or vendor selling or providing goods (e.g., tickets) or services (e.g., events) over the Internet. EX1005, 4:43-46, 5:39-42, 6:32-36. Promotional messages sent to users via the client can be "any advertising information related to a product or service that a client provides." *Id.*, 6:66-7:4, 17:56-58. Each such message is therefore a "third party message" associated with a third party ticket, service, or event provider. EX1003, ¶¶214-215.

c. Long discloses claims 4, 11, and 17

Long discloses **"configuring a service subscriber to receive additional content comprises configuring the service subscriber to receive, from one or more third party providers, third party messages comprising the at least one customized actionable item."** The click-to-text server confirms the subscription in message 222, stores "the user's subscription status associated with the client" in user

data 108, and thereafter “can provide service and/or send promotional messages 223 to the user.” EX1005, 8:6-21, 7:62-67; *see also id.*, 3:10-13, 6:48-52. Those messages come from one or more providers. Memory 103 stores “message data 107 (e.g., a set of promotional messages associated with a set of entities or clients)” and “client data 109 (e.g., user white list associated with a set of clients/entities).” *Id.*, 4:43-54.

The messages the subscriber receives include the customized actionable item. When the subscriber sends a purchase request, the server sends message 563, which “inform[s] the user of the shipping information and the payment information on file associated with the user” and “include[s] a link (‘checkout link’).” *Id.*, 15:56-66, Fig. 5G. A POSITA would have understood the server recording the subscription and then delivering the client’s messages to be “configuring” the subscriber to receive from third-party providers messages comprising the checkout link. EX1003, ¶¶216-218.

d. Long in view of Gaddis discloses claims 5, 12, and 18

Long and Gaddis render obvious “**the at least one customized actionable item comprises a secure link to perform the e-commerce transaction for purchasing tickets, merchandise, or products.**” As explained above, the “customized actionable item” is the encrypted PEL that the click-to-text server generated for the subscriber’s transaction and sent in message 563 as the “checkout

link.” *See supra* Section VII.A.4.c; EX1005, 15:62-66; EX1006, ¶¶34, 58-59. The subscriber fills a shopping cart on a website and taps the checkout link, and the server sends message 563 displaying “a shopping cart 503 with products 504 to be purchased” and a checkout link. EX1005, 15:56-66, 14:52-54, Figs. 5G-5H.

That link is a “secure link.” Gaddis’ PEL is “encrypted before sending to User and decrypted by OP to facilitate purchase,” and carries a “custhash” that is an “encrypted User identification (UserId) specific to the User.” EX1006, ¶¶34, 59; EX1003, ¶¶219-221.

For the reasons given in Section VII.A.3, incorporated here, a POSITA would have been motivated to secure Long’s checkout link with Gaddis’ encrypted PEL to protect the subscriber’s stored payment and shipping information, and would have had a reasonable expectation of success. EX1005, 12:67-13:5; EX1003, ¶¶222-223.

e. Long in view of Gaddis discloses claims 6, 13, and 19 obvious

Long in view of Gaddis discloses “**wherein the authentication information comprises an authentication cookie configured to be stored on an electronic device associated with the service subscriber**” obvious.

As noted in limitation 1[a], the “authentication information” in Long is the “user identifier” the subscriber’s mobile device supplies to the click-to-text server when the subscriber selects the “sign-up” link. *Supra* Section VII.A.4.b; EX1005, 8:55-59, 8:65-9:1. Long also discloses placing a cookie on the user device through

its integration tag. The tag “can be attached to a page load event at the user mobile device,” and on execution the device “generate[s] a unique visitor identifier and store[s] at least a portion of the integration tag in a local storage of the user mobile device, or as a cookie at the user mobile device.” *Id.*, 11:23-31, 11:46-50. The tag executes and “sends to the click-to-text server user data” including “user cookies” alongside “user phone number, user device identifier,” and other identifying information. *Id.*, 11:53-60. Long thus discloses a cookie on the user’s device that, when the tag fires at a merchant website, is sent to the server with user identification information. EX1003, ¶¶224-226.

To the extent Long does not expressly state that the user identifier comprises an authentication cookie, the combination of Long and Gaddis renders this claim obvious.

In Gaddis, the “User” is someone “whose identity has been previously verified by the Offer Provider,” which occurs after the User has logged into the website, saved their username and password on their device, “and/or is **verified by cookies** or other method well known by the skilled artisan (e.g. by the merchant via web browsers having saved their credentials).” EX1006, ¶61 (emphasis added). A POSITA would thus understand that Gaddis discloses a cookie residing on the User’s device as a record that the User was authenticated. *Id.*, ¶¶37, 61; EX1003, ¶¶227-

A POSITA would have been motivated to verify the subscriber from the cookie Long already returns to the server, so that the cookie serves as authentication information with the user identifier, as Gaddis discloses. EX1005, 7:43-48, 11:46-50, 11:53-60. A POSITA would have had a reasonable expectation of success: the modification uses a cookie Long already places at page load, and requires no new capability of the client server, the subscriber's device, or the click-to-text server. Gaddis confirms that verification by cookies is a "method well known by the skilled artisan." EX1006, ¶61. The result combines prior art elements according to known methods to yield predictable results. *See KSR*, 550 U.S. at 416; EX1003, ¶229.

f. Long discloses claims 7, 14, and 20

Long discloses that **"the third party message comprises"** an **"SMS message"** or **"MMS message."** Long's click-to-text server uses short-code or long-code cellular numbers, constructs an "sms:" link with an SMS body, and sends client messages through a wireless communication provider server such as AT&T. EX1005, 7:11-21, 9:45-10:65, 11:1-10. A POSITA would have understood that functionality to support "third party messages" comprising "an SMS message." EX1003, ¶230.

Long also discloses that second user interface displays a client's promotional images. EX1005, 16:40-46, Figs. 6A-6C. A POSITA would have concluded that

functionality supports “third party” “Multimedia Message Service (MMS) message[s].” EX1003, ¶¶231-232.

B. Ground 2: Claims 1-20 Are Obvious Over Louie alone or in View of Gaddis and the General Knowledge of a POSITA

1. Louie (EX1007)

U.S. Patent No. 10,360,627 to Louie et al., titled “Systems and Methods to Provide Account Features via Web Based User Interfaces” (“Louie”), issued July 23, 2019 from Application No. 14/106,380, filed December 13, 2013, and published June 19, 2014 as U.S. Patent Application Pub. No. 2014/0172660 A1. EX1007, Cover. Louie is assigned to Visa International Service Association and names a different inventive entity than the ’924 patent. *Id.*; EX1001, Cover. Both the filing and publication dates precede the ’924 patent’s September 27, 2018 priority date, so Louie is prior art under 35 U.S.C. § 102(a)(2). Neither the applicant nor the Examiner cited Louie during prosecution. EX1001, References Cited; EX1003, ¶234.

Louie describes a credit card portal that offers card benefits to cardholders. EX1007, 1:25-30, 3:49-4:11. Louie calls those benefits “account features” or “enhancement features” and defines them as “services or goods that a card issuer provides in addition to processing purchase transactions,” such as “extra warranty period and companion airline ticket.” EX1007, 1:47-61.

Cardholders reach the portal through a link on the credit card issuer's website. *Id.*, 24:21-30. The portal presents a customized page for each cardholder based on the user's identity. *Id.*

Cardholders use the portal to opt in to receive alerts about their card benefits at a phone number. In Figure 8, the cardholder enters “a mobile phone number and/or a phone number in entry boxes (221) to receive notifications,” and selects an option button “to request a notification be sent to the phone number specified in the entry box (221) associated with the text message whenever a feature benefit is available.” *Id.*, 13:1-15, Fig. 8. Louie's notification engine (117) then sends notifications and offers “via an email, a text/SMS message, a voice message.” *Id.*, 6:36-44, 9:8-14.

4 Notification		Email	Text Msg	Voice Msg
About				
Feature benefits	☐	☒ 223	☐	
Eligible for new features	☐	☒	☐	
Annual reminder	☐	☒	☐	
Address	Email	221		
	Text Message	221		
	Voice Message	221		
				Continue

FIG. 8

EX1007, Fig. 8 (annotated).

A cardholder who has opted in may then receive a text message when a benefit becomes available. In one example, the message reads, “You have made a purchase that is eligible for Sign and Travel Benefit. To activate the Benefit reply back with code ‘54367.’” *Id.*, 16:14-18. That “message is transmitted to a mobile phone of the account holder, which can reply to the message via short message service (SMS) to make the purchase.” *Id.*, 16:18-21. Alternatively, the cardholder may redeem the offer “by clicking on an ‘Activate’ link provided in the message,” which “brings the account holder to a page maintained by the web portal (143), where the details of the benefits can be explained and the benefit purchased.” *Id.*, 16:21-26. From that page, the cardholder “may select the user element (421) (‘Place Order’) to place the order of the account feature package.” *Id.*, 26:29-31, Fig. 24; EX1003, ¶¶235-244.

2. Gaddis (EX1006)

Gaddis is described in Section VII.A.2, *supra*, and is relied on in this ground as set out below.

3. Motivation to Combine Louie and Gaddis

A POSITA would have been motivated to combine Louie’s architecture for subscribing a cardholder at a telephone number, selecting offers from that cardholder’s purchase history, texting those offers, and routing the cardholder to a portal page built for that cardholder to buy, with Gaddis’ secure Promotionally Enabled Link (PEL) teaching. That combination takes advantage of Louie’s integrated offer messaging and customized webpage disclosures while incorporating

Gaddis' encryption techniques to keep cardholder account information confidential in e-commerce transactions. EX1003, ¶¶245.

Louie's own design choices would inform a POSITA that the link should be secured because Louie protects every point of access described to its portal. Before any account content appears, the issuer's website "verifies the identity of the user" and holds "one or more links (401) configured to refer the user to the portal (143) in a secure way." EX1007, 24:19-23. The portal authenticates that cardholder from "a parameter passed from the issuer site to portal (143) via the link (401)," and a cardholder who arrives without that handoff must "present a user name and a password to sign in." *Id.*, 24:59-66, 25:1-5. Louie sends API traffic over "a Secure Socket Layer (SSL) channel" and verifies "that the request message is from a system authorized to receive the requested data" before answering, *id.*, 22:28-34, and permits issuer customization only within "a predetermined set of parameters, but without the security vulnerability of unvalidated, uploaded HTML," *id.*, 24:2-6. A POSITA would thus expect that the "Activate" link Louie sends by SMS, which returns the cardholder to that same portal, would contain security measures as well. EX1003, ¶¶246-247.

Gaddis provides such measures. To prevent unwanted disclosure of the customer's information, Gaddis creates a link that includes an encrypted identifier "specific to the User" and encrypts that link "before sending to User." EX1006,

¶¶34, 59. That link may be an “SMS link,” and a User who selects text confirmation receives “a text message ... comprising the same PEL.” *Id.*, ¶¶8, 62. Gaddis is also built for systems like Louie’s: a sender may add its technique to a messaging operation already running, through software that “enables a merchant to incorporate programming code into their electronic communications” and a “module ... to encrypt and decrypt the UserIds as needed.” *Id.*, ¶¶60. The encrypted User ID applies across every deployment Gaddis describes: “In all scenarios, Users are assigned a unique User ID that may be provided to third party service providers” and that ID “is encrypted by methods well known in the art.” *Id.*, ¶52. That scenario fits Louie, whose portal is operated by the transaction handler rather than the issuer whose card is used. EX1007, 6:19-20; EX1003, ¶¶248-249.

A POSITA combining these teachings would have had a reasonable expectation of success. Louie and Gaddis are each analogous art to the ’924 patent. Each is in the same field of endeavor—using links delivered by SMS messaging to give a consumer access to customized webpages for completing online transactions—and each addresses the problem the ’924 patent identifies, that static webpages produce a cumbersome user experience that decreases a customer’s willingness and ability to complete e-commerce transactions. EX1001, Title, 1:16-18, 1:29-40, 1:66-2:1, 3:57-4:3. Louie builds its pages for the individual cardholder, “automatically generating and transmitting to the web browser of the user a

customized webpage” that “is customized by displaying an identification of the user,” presented “in a user friendly way” so the cardholder reaches the offer without hunting for it. EX1007, 40:31-41, 3:16-17, 25:57-58. Gaddis builds a page “specific to each User’s requirements” so the User buys “without entering any alpha numeric data.” EX1006, ¶¶8, 58; EX1003, ¶¶250-251.

The combination employs known methods to yield predictable results. Louie already authenticates users from credentials carried in issuer-website links and already handles encrypted traffic on its programming-interface channel. EX1007, 24:19-23, 24:59-66, 22:30-34. The modification puts an encrypted identifier into a different link pointing at that same portal, which Louie’s portal is equipped to resolve because it already identifies a credential out of a link and authenticates the cardholder from it. *Id.*, 24:59-66; EX1003, ¶252.

4. Independent Claim 1

a. Louie discloses 1[pre]

Louie discloses a **computer-implemented method**. Louie describes “a data processing apparatus, and more particularly a system to manage account features assigned to financial accounts that can be used to make payments for goods and services.” EX1007, 1:26-30. Its portal provides “access to the account feature data via a set of Application Programming Interfaces (APIs),” which let partners such as feature providers and issuers “build applications tailored to their needs and preferences, using the centralized account feature data.” EX1007, 2:64-3:3. Its

“computing apparatus” stores “account data ... identifying account features ... of a plurality of separate payment accounts,” receives “data identifying a first payment account,” and determines whether the account’s user “is eligible for a benefit of [an] account feature.” EX1007, 17:44-55.

A POSITA would have understood those disclosures to be a computer-implemented method performing the steps of claim 1. EX1003, ¶¶233, 253-254.

b. Louie alone or in view of Gaddis discloses 1[a]

Louie alone or in view of Gaddis discloses **configuring a service subscriber associated with a telephone number, to be subscribed to receive additional content at the telephone number, in response to determining that the service subscriber has previously provided authentication information.** Louie’s notification engine (117) markets additional purchases to the account holder through “a one-way or two-way communication,” and “communicate[s]” the notification “to the targeted account holder via an email, a text/SMS message, a voice message, etc.” EX1007, 9:5-12. Through the notification setup interface of Figure 8, “the account holder may provide the email address, a mobile phone number and/or a phone number in entry boxes (221) to receive notifications related to the events selected by the option buttons (e.g., 223).” *Id.*, 13:1-5, Fig. 8.

4 Notification		Email	Text Msg	Voice Msg
About				
Feature benefits		☐	☒ 223	☐
Eligible for new features		☐	☒	☐
Annual reminder		☐	☒	☐
Address	Email	221		
	Text Message	221		
	Voice Message	221		
Continue				

FIG. 8

The account holder “select[s] the option button (223) to request a notification be sent to the phone number specified in the entry box (221) associated with the text message whenever a feature benefit is available.” EX1007, 13:6-12. Those “selected preferences of the account holder are stored in the data warehouse (149) for the notification engine (117).” *Id.* Louie’s Figure 32 “‘My Account’ page” likewise lets the user “provide and/or update ... preferences related to the consumer account, such as the address, phone numbers, email address.” EX1007, 27:15-20, Fig. 32.

Louie’s portal “may require the user to present a user name and a password to sign in the portal (143) for accessing the account features of the consumer account of the user.” EX1007, 25:4-10. Alternatively, where the account holder arrives from the issuer’s website—which “verifies the identity of the user, before presenting the issuer content to the user”—the portal “authenticate[s] the user based on a parameter passed from the issuer site to portal (143) via the link (401).” *Id.*, 24:17-23, 24:59-

66. Figures 8 and 32 are portal interfaces for accessing and managing account features (i.e., notification preferences and account holder contact information), so they fall within the account-feature access that triggers this authentication requirement. The account holder must already have been authenticated before reaching the Figure 8 and Figure 32 interfaces where the account holder supplies a telephone number and elects to receive text-message notifications. *Id.*, 13:1-12, 27:15-20, Figs. 8, 32.

Back to Bank.com	How it Works	FAQ	Contact Us	My Account	My Inbox	Logout
----------------------------------	------------------------------	---------------------	----------------------------	----------------------------	--------------------------	------------------------

Card Benefits Welcome Lisa! 437  **Bank** 405

[Home](#) [My Benefits](#)

My Account Print

Please verify your profile information

Name Mr. ▾

Date of Birth 01 ▾ 01 ▾ 1901 ▾

Address:

 ▾

Time Zone: GTM (+8:00) ▾

Home Phone: Country ▾

Email:

Email Format Preference: ☒ Text ☐ HTML

Electronic Delivery **Term of Use:**

In this Authorization and Consent, the words I, ME, and MY mean each and all of those who apply for and/or use any of the electronic services described in this Disclosure and Agreement. The words YOU, YOUR, and YOURS ...

Electronic Disclosure option: ☐ Yes, send me electronic program disclosures ☒ No, do not send me electronic program disclosures

Email: Not Confirmed [Resend Confirmation Link](#)
 The disclosures will be electronically delivered to this email address

[Cancel](#)

FIG. 32

A POSITA would have understood Louie’s account holder to be the claimed service subscriber associated with a telephone number. The account holder supplies a telephone number and elects to receive text message notifications of feature benefits, and Louie stores that election “in the data warehouse (149) for the notification engine (117).” EX1007, 13:2-3, 27:15-19, Figs. 8, 32. That subscription is configured in response to determining the subscriber previously provided authentication information. The interface for making the election sits inside Louie’s portal, which the account holder reaches only after presenting a user name and password. EX1007, 24:19-20, 24:59-65, 25:3-4, 27:15-20; EX1003, ¶¶255-259.

Even if Louie did not disclose that the configuration occurs in response to determining that the subscriber has previously provided authentication information, Gaddis does. Gaddis describes a need in the art “to authenticate the User prior to sending the advertisement,” and defines “User” as a cardholder “who receives promotional offers due to authentication through previous registration, account creation and opt in for promotions from Offer Provider.” EX1006, ¶¶5, 37. That “[p]rior verification occurs in situations wherein the User has already logged into the merchant’s website, has saved their username and password on their electronic communications device, and/or is verified by cookies or other method well known by the skilled artisan.” *Id.*, ¶61.

A POSITA would be motivated to combine Louie and Gaddis for this purpose. Louie's issuer website "verifies the identity of the user" before showing account content, and the portal then authenticates that cardholder from "a parameter passed from the issuer site to portal (143) via the link (401)." EX1007, 24:17-23, 24:59-66. The cardholder sets notification preferences during that authenticated session, and Louie's offers go to a cardholder "who had previously given permission to receive promotional offers." *Id.*, 13:1-15, 16:14-22, Fig. 8. Gaddis defines its "User" by that same opt-in, sent only "due to authentication through previous registration." EX1006, ¶37; *see also id.*, ¶51 (the User "must have a 'pre-existing' account with the merchant," whose billing and contact information the merchant "must have previously acquired"). In the combination, the cardholder subscribes through Louie's portal, and the portal sends the offer only after confirming the cardholder opted in and was already verified. EX1003, ¶¶256-261.

A POSITA would have been motivated to make this combination to confirm that any text message with a link to the user's account reaches only a verified user, both for security and to ensure billing information is on file for a seamless purchase. This combines prior art elements according to known methods to yield predictable results, and uses a known technique to improve a similar method in the same way. *Supra* Section VII.B.3. Because Louie's portal already authenticates user accounts and manages billing information, verifying that the phone number belongs to the

cardholder before sending the linked message is a reasonable modification. EX1007, 24:17-23, 24:59-66; EX1003, ¶¶261.

c. Louie alone or in view of Gaddis discloses 1[b]

Louie alone or in view of Gaddis discloses **“activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction, the activating comprising generation of secure access information for performing the e-commerce transaction.”**

Specifically, Louie’s portal generates a webpage for the individual cardholder (the “customized webpage”). Louie claims “automatically generating and transmitting to the web browser of the user a customized webpage” that “is separate from the website of the issuer” and “is customized by displaying an identification of the user and the white label resources” of that issuer. EX1007, 40:32-38. The specification describes the same operation: when the user is referred to the portal by the issuer’s website, “the identity of the issuer is used to generate a customized presentation of the user interfaces,” using “configurable white label resources and/or custom HTML code specified for the issuer.” *Id.*, 23:43-50. Those resources—“logo, label, text area and links”—apply the issuer’s branding to the page the portal builds for the individual cardholder. *Id.*, 28:31-32. When the cardholder reaches the portal, it “presents a user interface customized based on the identity of the issuer and/or the user.” *Id.*, 24:23-26.

Louie discloses a “customized actionable item” included in that webpage. Louie’s system sends the cardholder a message identifying a benefit the cardholder is eligible to purchase: “You have made a purchase that is eligible for Sign and Travel Benefit. To activate the Benefit reply back with code ‘54367.’” EX1007, 16:14-18. The cardholder receives that message on a mobile phone and may purchase the benefit by replying via short message service (SMS) or “by clicking on an ‘Activate’ link provided in the message,” which “brings the account holder to a page maintained by the web portal (143), where the details of the benefits can be explained and the benefit purchased.” *Id.*, 16:19-29. A POSITA would understand that “Activate” link to be a “customized actionable item for performing an e-commerce transaction.” It is specific to the benefit for which the cardholder’s own prior purchase made the cardholder eligible, and it opens the portal page where that benefit is purchased. *Id.*, 16:22-26; EX1003, ¶¶262-263.

Louie discloses activating the customized webpage “comprising generation of secure access information.” Louie’s issuer website “verifies the identity of the user, before presenting the issuer content to the user,” and contains “one or more links (401) configured to refer the user to the portal (143) in a secure way.” EX1007, 24:17-23, Fig. 19. The portal then “authenticate[s] the user based on a parameter passed from the issuer site to portal (143) via the link (401).” *Id.*, 24:59-66. Louie applies the same discipline to its other channel, routing application requests over “a

Secure Socket Layer (SSL) channel” and verifying “that the request message is from a system authorized to receive the requested data.” *Id.*, 22:30-36. A POSITA would understand that the “Activate” link within the SMS message carries the same security. Louie secures every other path into the portal, and the page that “Activate” link opens is one where account features are purchased. *Id.*, 16:24-26. A POSITA generating a link that reaches a cardholder’s account and stored billing information would have secured that link as a matter of routine design, particularly because the art recognized that SMS without such security features could expose sensitive user data. EX1003, ¶¶264-267. Encrypting such a link was a well-known technique a POSITA could readily implement. *Id.*

Even if Louie did not disclose this limitation, Gaddis does. As discussed in Ground 1 limitation 1[b], incorporated herein by reference, Gaddis’ “electronic message generation module 408” transmits messages “comprising encrypted links unique to each User”—Promotionally Enabled Links (PEL)—which a POSITA would understand to be “secure access information.” EX1006, ¶53; EX1003, ¶¶268; *supra* Section VII.A.4.c.

A POSITA would recognize Louie could be modified so its SMS “Activate” link—the customized actionable item—incorporates the security characteristics of Gaddis’ PEL. Louie’s portal (143) would build that link as a PEL from a merchant identifier, a deal identifier, and an encrypted user identifier, encrypt it before

transmission, and generate from that same information the benefit page the link opens. EX1007, 16:19-29; EX1006, ¶¶34, 57-59. When the cardholder selects the link, the portal decrypts it, resolves the encrypted user identifier against the account and billing information it maintains, and re-directs the cardholder to “a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User”—the purchase page for that benefit. EX1006, ¶59; EX1007, 16:24-29; EX1003, ¶269.

A POSITA would have been motivated to make this combination to achieve the security objectives Louie already states. Louie authenticates the other paths into the portal and uses links to refer the user to the portal “in a secure way.” EX1007, 24:17-23. Gaddis’ encrypted PEL carries a user-specific encrypted identifier that the server decrypts to build the user’s webpage, furthering that objective for the one path Louie leaves unsecured. EX1007, 24:17-23, 24:59-66, 22:30-36; EX1006, ¶¶34, 58-59. For the reasons given for the Long-Gaddis combination, this combines prior art elements according to known methods to yield predictable results, and uses a known technique to improve a similar method in the same way. A POSITA would also have had a reasonable expectation of success, because Gaddis expressly defines its PEL as an “email link, SMS link, or link posted on a User’s social media site” confirming it could be used for Louie’s SMS “Activate” link. *Supra* Section VII.B.4.c; EX1006, ¶¶39, 62; EX1003, ¶270.

d. Louie discloses 1[c]

Louie discloses **wherein the at least one customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber.** As discussed for 1[b], Louie’s “Activate” link that opens a portal page where a cardholder benefit is purchased is the claimed “customized actionable item.” EX1007, 16:19-29. Louie triggers the SMS message including that link based on the cardholder’s own prior transactions. EX1003, ¶271.

Louie’s system triggers additional transactions “in response to certain transactions qualifying for offers associated with account features.” EX1007, 3:49-55. Its feature offer engine uses “the account information and/or purchase history to determine or identify a particular account holder based on some predetermined criteria”—for example, “account holders with an annual spend in the travel category of \$30,000 who have also purchased at least one trip cancellation insurance within the last two years.” *Id.*, 8:46-52. So a cardholder who buys an airline ticket qualifying for premium trip-cancellation coverage, on an account lacking that feature, is notified “to enroll in the account feature.” *Id.*, 3:59-66. A trigger may also be an “aggregated spending threshold” or “a predetermined [number] of transactions in a category.” *Id.*, 9:59-10:10, 10:63-11:3, Figs. 11, 13.

The resulting message can be an SMS that includes the “Activate” link. Louie’s notification engine (117) notifies the account holder “via an email, a text

message, a voice message, etc., when a transaction of the account holder qualifies for the benefit of a feature (e.g., 127).” *Id.*, 6:38-45. Louie markets the applicable feature “via the notification engine (117) after a cardholder’s purchase of a qualifying transaction,” and that “qualifying transaction triggers One-on-One marketing to the cardholder for the appropriate ‘Feature.’” *Id.*, 7:63-8:5.

A POSITA would thus have understood Louie’s “Activate” link to correspond to prior actions associated with the cardholder’s prior transactions. Louie generates the link after a triggering event—the cardholder’s prior purchase, aggregated spending, or number of prior transactions satisfying a feature rule—delivers it in a message identifying that qualifying purchase, and opens from it a page for purchasing the benefit for which the cardholder is thereby eligible. EX1007, 3:49-66, 8:46-52, 9:59-10:10, 16:14-29; EX1003, ¶¶272-274.

e. Louie discloses 1[d]

Louie discloses “**generating, for the service subscriber, a third party message associated with the one or more customized webpages, the third party message including the at least one customized actionable item.**” Louie’s notification engine (117) generates a message to the account holder describing the qualifying account feature and including an “Activate” link or code, communicated “via an email, a text/SMS message, a voice message, etc.” EX1007, 9:5-12, 16:4-23. That message comes from the issuer or feature provider behind the account feature—

a party distinct from the account holder and from Louie’s notification engine and portal, which perform the claimed steps. *Id.* Louie’s feature providers and issuers supply and administer those features through the portal’s APIs and a “self service module.” EX1007, 2:64-3:8, 13:1-12, 14:38-46. A POSITA would thus have understood that notification, with its link to the 1[b] customized webpage, to be a third party message associated with that webpage and including the customized actionable item. EX1003, ¶275.

f. Louie discloses 1[e]

Louie discloses “**causing transmission of the generated third party message to the service subscriber.**” As discussed for 1[d], Louie’s notification engine (117) generates that message and transmits it to the account holder’s phone number on file “via an email, a text/SMS message, a voice message, etc.” Louie confirms the offer “message is transmitted to a mobile phone of the account holder.” *See supra* Section VII.B.4.e; EX1007, 9:5-12, 13:1-12, 16:4-23, 16:19-21; EX1003, ¶276.

5. Independent Claims 8 and 15

Claim 8 recites “**a system comprising a processor and memory configured to store program instructions, wherein, when executed by the processor, the program instructions cause the processor to perform operations comprising**” the same five operations recited in claim 1, and claim 15 recites a “**non-transitory computer-readable storage medium for use in conjunction with a computer, the**

computer-readable storage medium storing program instructions that, when executed by the computer, cause the computer to carry out one or more operations comprising” those same five operations. The body limitations of claims 8 and 15 correspond to 1[a] through 1[e], with one exception addressed below. Louie in view of Gaddis therefore discloses 8[c] through 8[g] and 15[a] through 15[e] for the reasons given above for 1[a] through 1[e], respectively. *See supra* Sections VII.B.4.b-VII.B.4.f; EX1003, ¶277.

With respect to 8[pre], Louie discloses “[a] **system comprising.**” EX1003, ¶278. Louie’s “embodiments of the present disclosure relate to a data processing apparatus, and more particularly a system to manage account features assigned to financial accounts that can be used to make payments for goods and services.” EX1007, 1:25-30. Louie provides “systems and methods ... to trigger further transactions in response to certain transactions qualifying for offers associated with account features.” EX1007, 3:49-59. Figure 1 depicts that system’s components:

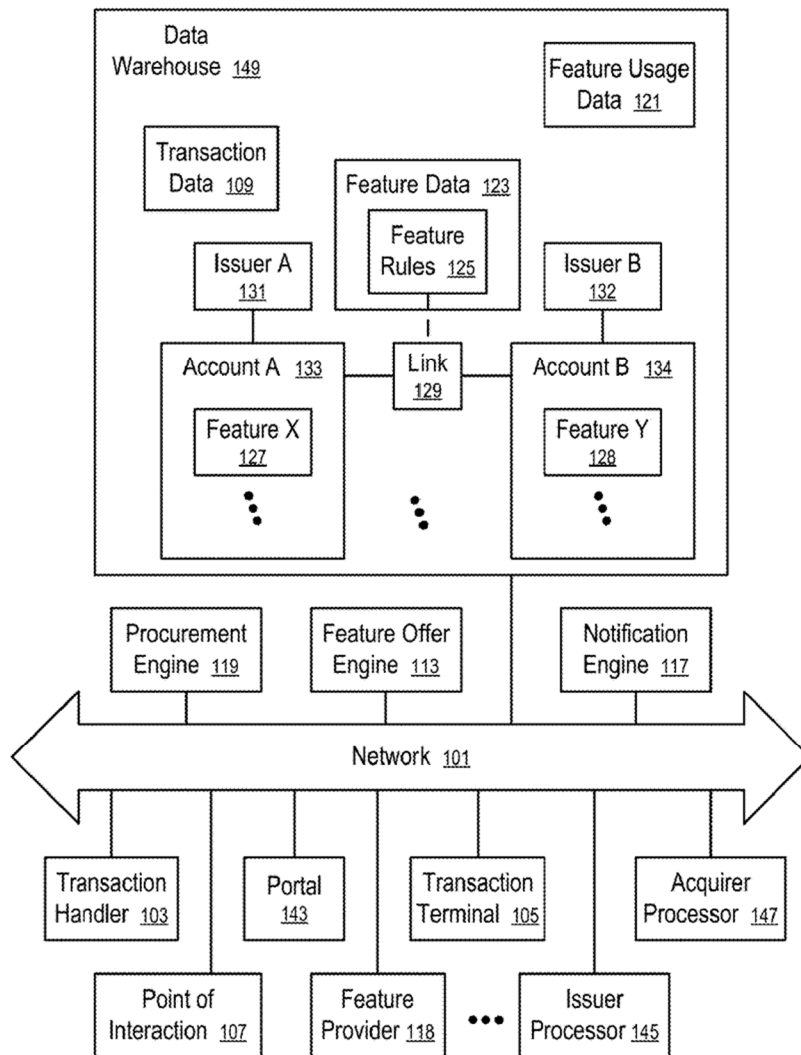


FIG. 1

As to 8[a] and 8[b], Louie discloses “a processor” and “memory configured to store program instructions, wherein, when executed by the processor, the program instructions cause the processor to perform operations comprising” the same five operations recited in claim 1. EX1003, ¶279. Louie’s “computing apparatus includes at least one processor (e.g., 173), and a memory (e.g., 167, 179) storing instructions configured to instruct the at least one processor to perform

operations discussed herein.” EX1007, 28:62-65. Its data processing system likewise “interconnects a microprocessor(s) (173) and memory (167),” with the microprocessor “coupled to cache memory (179).” EX1007, 37:43-64, Fig. 17, cl. 10.

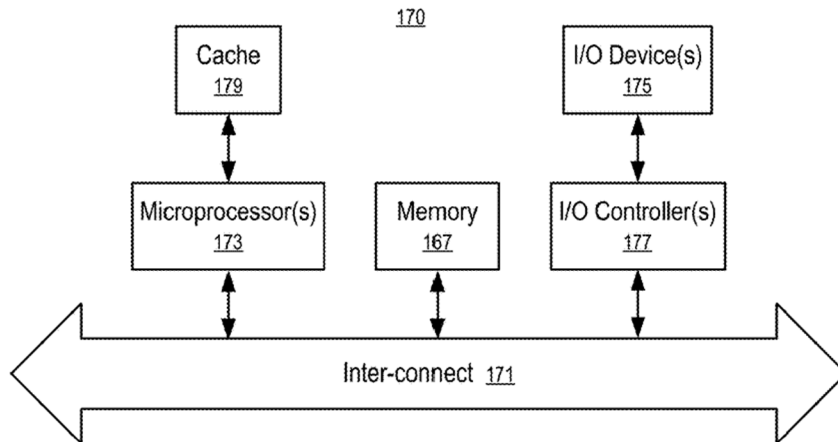


FIG. 17

With respect to 15[pre], Louie discloses “[a] **non-transitory computer-readable storage medium for use in conjunction with a computer, the computer-readable storage medium storing program instructions that, when executed by the computer, cause the computer to carry out one or more operations comprising,**” for the reasons given for 1[pre] and 8[pre] through 8[b]. *See supra* Sections VII.B.4.a, VII.B.5; EX1003, ¶280. Louie’s “machine readable medium can be used to store software and data which when executed by a data processing system causes the system to perform various methods,” and that software

and data “may be stored in various places including for example ROM, volatile RAM, non-volatile memory and/or cache.” EX1007, 38:63-39:1.

Limitation 15[b] combines 1[b] with the subject matter claim 2 adds to claim 1. It recites limitation 1[b]’s activating step and adds that the e-commerce transaction is “to purchase tickets, merchandise, or products or view the one or more customized webpages depicting information about the tickets, merchandise, or products.” EX1001, 20:66-21:3, 22:25-28. Louie and Gaddis render each element obvious for the reasons given for 1[b] and for claims 2 and 9. Louie’s “Activate” link opens the portal page where the cardholder buys the account feature. Gaddis’ encryption secures that link. A POSITA would thus have understood that Louie and Gaddis meet 15[b]. *See supra* Section VII.B.4.c; *infra* Section VII.B.6.a; EX1003, ¶281. Thus, Louie in view of Gaddis renders claims 8 and 15 obvious. EX1003, ¶282.

6. Dependent Claims

Each claim addressed below depends from claim 1, claim 8, or claim 15. As shown above, Louie in view of Gaddis discloses every limitation of those independent claims. *See supra* Sections VII.B.4-VII.B.5. The discussion below addresses only the feature each dependent claim adds.

a. Louie discloses claims 2 and 9

Claims 2 and 9 add that “**the at least one customized actionable item comprises data to access the one or more customized webpages, the data being**

configured to enable the service subscriber to purchase tickets, merchandise, or products or view the customized webpages depicting information about the tickets, merchandise, or products.” Louie discloses these limitations.

As discussed for claim 1, Louie’s “Activate” link is the “customized actionable item.” Clicking it “brings the account holder to a page maintained by the web portal (143), where the details of the benefits can be explained and the benefit purchased,” and from that page the cardholder “may select the user element (421) (‘Place Order’) to place the order of the account feature package.” EX1007, 16:22-26, 26:29-31, Fig. 24.

Louie’s “Activate” link data enables the account holder to reach the web-portal page to purchase an airline ticket feature or view its details. A POSITA would thus have understood that data to access the customized webpage and to enable the service subscriber to purchase tickets, merchandise, or products or view pages depicting information about them. EX1003, ¶¶283-285.

b. Louie discloses claims 3, 10 and 16

Claims 3, 10, and 16 add that **“the third party message is associated with a third party ticket provider, a third party service provider, or a third party event provider.”** Louie discloses this limitation.

As discussed for 1[d], Louie’s notification engine generates the third party message on behalf of the issuer or feature provider. *See supra* Section VII.B.4.e.

Louie’s portal “provide[s] access to the account feature data via a set of Application Programming Interfaces (APIs),” which “allow[] a partner, such as a feature provider, an issuer, ... to build applications tailored to their needs and preferences.” EX1007, 2:64-3:8, 5:42-59. Those partners come from a network of approved feature providers and vendors who supply features or act as service providers and issuers, and issuers “administer account features ... through a self service module.” *Id.*, 12:14-17, 14:38-46, 15:53-16:2. Louie’s premium trip cancellation coverage, sold against an airline-ticket purchase, confirms that those providers include ticket-related service providers. *Id.*, 3:60-66, 8:46-52.

A POSITA would thus have understood Louie’s feature providers, issuers, and approved vendors—who supply and administer features such as trip cancellation coverage tied to an airline ticket through the API-accessible portal—to be third party ticket providers or third party service providers. EX1003, ¶¶286-288.

c. Louie discloses claims 4, 11, and 17

Claims 4, 11, and 17 add that “**configuring a service subscriber to receive additional content comprises configuring the service subscriber to receive, from one or more third party providers, third party messages comprising the at least one customized actionable item.**” Louie discloses this limitation.

As discussed for 1[a], Louie’s account holder selects notification preferences and a phone number through the Figure 8 interface to receive messages about feature

benefits. *See supra* Section VII.B.4.b; EX1007, 13:1-12, Fig. 8. The account holder “select[s] the option button (223) to request a notification be sent to the phone number specified in the entry box (221) ... whenever a feature benefit is available to the account holder,” and Louie stores those “selected preferences ... in the data warehouse (149) for the notification engine (117).” *Id.*, 13:6-12, 13:49-52, Fig. 8. Louie further discloses that “issuers ... are to administer account features ... through a self service module,” and that account holder messages sent via the notification engine include an “Activate” link comprising the customized actionable item discussed for limitations 1[b] and 1[d]. EX1007, 14:38-46, 16:4-16:23.

A POSITA would have understood that when the cardholder sets his notification preferences, he is causing Louie’s notification engine (117) to configure his account to receive messages that will include offers from third party providers with the customized actionable item. EX1003, ¶¶289-291.

d. Louie alone or in view of Gaddis discloses claims 5, 12, and 18

Claims 5, 12, and 18 add that **“the at least one customized actionable item comprises a secure link to perform the e-commerce transaction for purchasing tickets, merchandise, or products.”** Louie renders this limitation obvious alone or in view of Gaddis.

Louie’s disclosures identified for 1[b] establish that its “Activate” link is a “secure link.” *See supra* Section VII.B.4.c. Louie secures every path into the portal:

users reach it “in a secure way,” are authenticated “based on a parameter passed from the issuer site to portal (143) via the link (401),” and requests travel over “a Secure Socket Layer (SSL) channel.” EX1007, 16:19-29, 22:28-39, 24:17-23, 24:59-66. A POSITA would accordingly have understood that the “Activate” link that opens the cardholder’s purchase page carries that same secure access information. EX1003, ¶¶292-293.

Even if Louie did not disclose this limitation, Gaddis does. For the reasons given for 1[b], a POSITA would have modified Louie’s “Activate” link to incorporate the security characteristics of Gaddis’ Promotionally Enabled Link. *See supra* Section VII.B.4.c. Under that combination, the “customized actionable item” is the encrypted PEL that Louie’s portal generates for the cardholder’s offer and sends as the “Activate” link. That PEL is a “secure link” because it is “encrypted before sending to User and decrypted by OP to facilitate purchase” and carries a “custhash” that is an “encrypted User identification (UserId) specific to the User.” EX1006, ¶¶34, 59; EX1007, 16:19-29. The motivation, known-technique rationale, and reasonable expectation of success set forth above apply equally here. *See supra* Section VII.B.3; EX1003, ¶294.

e. Louie in view of Gaddis discloses claims 6, 13, and 19

Claims 6, 13, and 19 add that **“the authentication information comprises an authentication cookie configured to be stored on an electronic device**

associated with the service subscriber.” Louie in view of Gaddis renders this limitation obvious.

As noted for 1[a], the “authentication information” in Louie is the credential by which the portal (143) authenticates the account holder before the holder reaches the notification and account-preference interfaces of Figures 8 and 32. That credential is either the “user name and a password” the portal may require “to sign in the portal (143),” or the “parameter passed from the issuer site to portal (143) via the link (401)” from which the portal “automatically authenticate[s] the user.” *Supra* Section VII.B.4.b; EX1007, 13:1-12, 24:59-66, 25:4-10, 27:15-20, Figs. 8, 32. To the extent Louie does not expressly state that this authentication information comprises an authentication cookie, a POSITA would have found the cookie limitation obvious in view of Gaddis. EX1003, ¶¶295-297.

Gaddis “User” is someone “whose identity has been previously verified by the Offer Provider.” EX1006, ¶61. That “[p]rior verification occurs in situations wherein the User has already logged into the merchant’s website, has saved their username and password on their electronic communications device, and/or is *verified by cookies* or other method well known by the skilled artisan (e.g. by the merchant via web browsers having saved their credentials).” *Id.* (emphasis added). A POSITA would thus understand Gaddis to disclose a cookie residing on the User’s device as a record of that authentication. *Id.*, ¶¶37, 61; EX1003, ¶298.

A POSITA would have been motivated to use Gaddis cookie-based verification as the authentication information in Louie’s system, with a reasonable expectation of success. Gaddis describes verification by cookies as a “method well known by the skilled artisan,” and Louie already authenticates the cardholder “based on a parameter passed from the issuer site to portal (143) via the link (401)” so that “[t]he user does not have to provide another set of credential [sic] to sign in the portal (143).” EX1006, ¶61; EX1007, 24:59-66. Recording that earlier authentication in a cookie on the device serves the purpose Louie describes—reducing friction in reaching the account feature—and requires no new components or message steps. Gaddis confirms that a conventional browser mechanism does it. EX1003, ¶299. Further, the motivation and reasonable expectation of success set forth above apply here. *See supra* Section VII.B.3.

f. Louie discloses claims 7, 14, and 20

Claims 7, 14, and 20 add that **“the third party message comprises a Short Message Service (SMS) message or a Multimedia Message Service (MMS) message.”** Louie discloses this limitation.

As discussed for 1[d] and 1[e], Louie transmits the “third party message” as a “text/SMS message” carrying an “Activate” link to an account feature. EX1007, 9:5-12, 16:4-23; *see supra* Sections VII.B.4.e-VII.B.4.f. A POSITA would thus have understood that message to comprise an SMS message. EX1003, ¶¶300-301.

VIII. MANDATORY NOTICES

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

Petitioner Intuit Inc. is the real party-in-interest. Further, Petitioner certifies that no other party exercised control or could have exercised control over, or contributed to any funding of, the preparation or filing of this Petition. Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney is attached hereto.

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

Petitioner is aware of the following related matters. Patent Owner asserts U.S. Patent Nos. 12,368,799 and 11,876,924 against Petitioner in *IQX Corp. v. Intuit Inc.*, No. 2:26-cv-00351-JRG-RSP (E.D. Tex., filed Apr. 30, 2026). Petitioner is concurrently filing a petition for *inter partes* review of U.S. Patent No. 12,368,799, which issued from an application in the '924 patent's priority chain.

Patent Owner also asserts U.S. Patent Nos. 12,368,799 and 11,876,924 against Salesforce, Inc. in *IQX Corp. v. Salesforce, Inc.*, No. 7:26-cv-00213-DC-DTC (W.D. Tex., filed May 28, 2026). Salesforce has filed four petitions for *inter partes* review involving iQX Corp: *Salesforce, Inc. v. IQX Corp.*, IPR2026-00475 (P.T.A.B., filed Sept. 24, 2026), challenging U.S. Patent No. 12,368,799; *Salesforce, Inc. v. IQX Corp.*, IPR2026-00476 (P.T.A.B., filed Sept. 24, 2026), challenging U.S. Patent No. 11,876,924; *Salesforce, Inc. v. IQX Corp.*, IPR2026-00477 (P.T.A.B., filed Sept. 24, 2026), challenging U.S. Patent No. 12,20,0165; and *Salesforce, Inc. v. IQX Corp.*,

IPR2026-00478 (P.T.A.B., filed Sept. 24, 2026), challenging U.S. Patent No. 12,438,978.

C. Designation of Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3)) and Service of Information (37 C.F.R. § 42.8(b)(4))

Petitioner designates Jessica L. Benzler (Reg. No. 73,137) as lead counsel and Michael J. Sacksteder (*pro hac vice* forthcoming), Daniel Ledesma (*pro hac vice* forthcoming), Blaine Schmidt (*pro hac vice* forthcoming), and Geoffrey R. Miller (*pro hac vice* forthcoming) as backup counsel.

Service of any documents may be made to:

FENWICK & WEST LLP
One Front Street, 33rd Floor
San Francisco, CA 94111
Tel: (415) 875-2300
Fax: (650) 938-5200
Email: intuit-ixx@fenwick.com
jbenzler@fenwick.com
msacksteder@fenwick.com
dledesma@fenwick.com
bschmidt@fenwick.com
gmler@fenwick.com

D. Fees for *Inter Partes* Review (37 C.F.R. § 42.15(a))

The Director is authorized to charge the fee specified by 37 C.F.R. § 42.15(a) to Deposit Account No. 19-2555.

Dated: October 19, 2026

Respectfully submitted,

FENWICK & WEST LLP

/Jessica L. Benzler/

Jessica L. Benzler

Reg. No. 73,137

Attorneys for Petitioner

Intuit Inc.

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION**

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this Petition complies with the 14,000 word type-volume limitation. The Petition contains 13,998 words, excluding the parts of the Petition exempted from the type-volume limitation.

Dated: October 19, 2026

FENWICK & WEST LLP

/Jessica L. Benzler/

Jessica L. Benzler

Reg. No. 73,137

Attorneys for Petitioner

Intuit Inc.

**CERTIFICATION OF SERVICE ON PATENT OWNER
(37 C.F.R. § 42.105)**

The undersigned hereby certifies that the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 11,876,924 and accompanying Exhibits 1001-1032 are being sent via Federal Express – Priority Delivery on October 19, 2026, upon Patent Owner by serving the correspondence address of record with the USPTO as follows:

105822 – Aurora Consulting LLC
Ashley Sloat
810 Cottageview Drive, Suite G10
Traverse City, MI 49684

Further, a courtesy copy of this Petition for *Inter Partes* Review was sent via Federal Express to Patent Owner’s litigation counsel:

Reza Mirzaie
Marc A. Fenster
Christian Conkle
Russ August & Kabat
12424 Wilshire Blvd., 12th Floor
Los Angeles, CA 90025

FENWICK & WEST LLP

/Jessica L. Benzler/

Jessica L. Benzler

Reg. No. 73,137

Attorneys for Petitioner

Intuit Inc.