

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. IPR2026-0017
Patent 11,876,924 B2

**DECLARATION OF BENJAMIN B. BEDERSON, PH.D. IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 11,876,924**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	6
II. BACKGROUND AND QUALIFICATIONS	6
III. COMPENSATION AND RELATIONSHIP WITH PARTIES.....	15
IV. MATERIALS CONSIDERED	15
V. BASIS OF OPINIONS FORMED	19
A. Level of Ordinary Skill in the Art	19
VI. THE '924 PATENT	20
A. Purported Invention of the '924 Patent	21
B. Prosecution History	32
VII. CLAIM CONSTRUCTION	37
A. Legal Standard for Claim Construction	37
VIII. OBVIOUSNESS STANDARD.....	37
IX. ANALYSIS OF THE TECHNICAL BASIS UNDERLYING THE GROUNDS OF REJECTION SET FORTH IN THE PETITION FOR <i>INTER PARTES</i> REVIEW.....	41
A. State of the Art	41
1. Configuring Subscriptions Associated With Customers' Phone Numbers and SMS-Based Marketing	42
2. User Authentication, Secure Links, and Cookies	45
a. Cookies	47
b. Secure Links	48
3. Customized Web Pages.....	50

4.	Interactive Elements that Enable Purchasing of Products Tailored to the Consumer's Interests	52
B.	Specific References that Render the Claims Obvious	54
1.	Secondary Considerations.....	54
C.	Ground 1: Claims 1-20 Are Rendered Obvious by Long in View of Gaddis and the General Knowledge of a POSITA	54
1.	U.S. Patent No. 11,553,074 to Long.....	54
2.	U.S. Patent Application Publication No. 2012/0310752 to Gaddis	63
3.	Motivation to Combine Long with Gaddis	71
4.	Independent Claim 1	77
a.	Long Discloses 1[pre].....	77
b.	Long Discloses 1[a]	78
c.	Long in View of Gaddis Discloses 1[b]	82
d.	Long Discloses 1[c]	92
e.	Long Discloses 1[d].....	93
f.	Long Discloses 1[e]	95
5.	Independent Claims 8 and 15.....	96
a.	Independent Claim 8.....	96
(1)	Long discloses 8[pre].....	96
(2)	Long discloses 8[a]	96
(3)	Long discloses 8[b].....	96
(4)	Long discloses 8[c]	96
(5)	Long and Gaddis render 8[d] obvious	97
(6)	Long discloses 8[e]	97

(7)	Long discloses 8[f]	97
(8)	Long discloses 8[g].....	97
b.	Independent Claim 15.....	97
(1)	Long discloses 15[pre].....	97
(2)	Long discloses 15[a].....	98
(3)	Long and Gaddis render 15[b] obvious	98
(4)	Long discloses 15[c].....	99
(5)	Long discloses 15[d].....	99
(6)	Long discloses 15[e].....	99
6.	Dependent Claims	99
a.	Long Discloses Claims 2 and 9	99
b.	Long Discloses Claims 3, 10, and 16	101
c.	Long Discloses Claims 4, 11, and 17	102
d.	Long in View of Gaddis Discloses Claims 5, 12, and 18.....	103
e.	Long in View of Gaddis Discloses Claims 6, 13, and 19.....	104
f.	Long Discloses Claims 7, 14, and 20	107
D.	Ground 2: Claims 1-20 Are Rendered Obvious by Louie in View of Gaddis and the General Knowledge of a POSITA	107
1.	U.S. Patent No. 10,360,627, titled “Systems and Methods to Provide Account Features via Web Based User Interfaces” to Anne Marie Louie et al.....	108
2.	Motivation to Combine Louie with Gaddis	113
3.	Independent Claim 1	119
a.	Louie Discloses 1[pre].....	119

b.	Louie Discloses 1[a]	120
c.	Louie in View of Gaddis Discloses 1[b]	126
d.	Louie Discloses 1[c]	131
e.	Louie Discloses 1[d]	133
f.	Louie Discloses 1[e]	134
4.	Independent Claims 8 and 15	134
5.	Dependent Claims	139
a.	Louie Discloses Claims 2 and 9	139
b.	Louie Discloses Claims 3, 10, and 16	140
c.	Louie Discloses Claims 4, 11, and 17	141
d.	Louie in View of Gaddis Discloses Claims 5, 12, and 18	142
e.	Louie in View of Gaddis Discloses Claims 6, 13, and 19	143
f.	Louie Discloses Claims 7, 14, and 20	146
X.	CONCLUSION	146

I, Benjamin B. Bederson, Ph.D., declare as follows:

I. INTRODUCTION

1. I have been asked by the party requesting this review, Intuit Inc. (“Petitioner”), to provide my expert opinions in support of the above-captioned petition for *inter partes* review of U.S. Patent No. 11,876,924 (the “’924 patent” or the “challenged patent”), challenging the patentability of claims 1-20 of the ’924 patent.

2. I currently hold the opinions set forth in this declaration.

3. In summary, it is my opinion that the references cited and discussed below render obvious the challenged claims of the ’924 patent. My detailed opinions on the claims are set forth below.

II. BACKGROUND AND QUALIFICATIONS

4. In the paragraphs below, I provide a summary of my qualifications. My curriculum vitae, which includes a more detailed summary of my background, experience, and publications, is attached as EX1004.

5. I received a Bachelor of Science degree in Computer Science with a minor in Electrical Engineering from Rensselaer Polytechnic Institute (“RPI”) in 1986. I received a Master of Science degree and a Ph.D. in Computer Science from New York University (“NYU”) in 1989 and 1992, respectively.

6. Since 1998, I have been a Professor of Computer Science at the University of Maryland (“UMD”), where I have had joint appointments at the Institute for Advanced Computer Studies and the College of Information Studies (Maryland’s “iSchool”) and am currently Professor Emeritus. I was also Associate Provost of Learning Initiatives and Executive Director of the Teaching and Learning Transformation Center from 2014 to 2018. I am a member and previous director of the Human-Computer Interaction Lab (“HCIL”), the oldest and one of the best known Human-Computer Interaction (“HCI”) research groups in the country.

7. For more than 30 years, I have studied, designed, and worked in the field of computer science and human-computer interaction. My experience includes 30 years of teaching and research, with research interests in human-computer interaction and the software and technology underlying today’s interactive computing systems. This includes the design and implementation of user interfaces and software applications using a wide range of technologies including web servers and websites, databases, embedded systems, and mobile devices, including smart phones and PDAs.

8. I was co-founder and Chief Scientist of Zumobi, Inc. from 2006 to 2014, a Seattle-based startup that is a publisher of content applications and advertising platforms for smartphones. Zumobi was a VC-funded startup for

mobile apps and advertising. I served as its VP Client Technologies from September 2006 to January 2008 and as its Chief Scientist from January 2008 to October 2014. Zumobi created its own advertising platform called Zumobi Brand Integration (ZBi) that included both the ability to incorporate third party advertisements as well as include its own. The platform included the ability to have links from ads to associated content as well as links to ads. Users could share advertisements with friends and include user generated content with the ads. All of these user engagement interactions were tracked.

9. I am also co-founder and co-director of the International Children's Digital Library ("ICDL"), a web site launched in 2002 that provides the world's largest collection of freely available online children's books from around the world with an interface aimed to make it easy for children and adults to search and read children's books online. I was also co-founder and prior Chief Technology Officer of Hazel Analytics from 2014 to 2023, a data analytics company. In addition, I have for more than 25 years consulted for numerous companies in the area of user interfaces, including EPAM, Lockheed Martin, Logitech, Microsoft, NASA Goddard Space Flight Center, the Palo Alto Research Center, and Sony.

10. At UMD, my research has been in the area of HCI, a field that relates to the development and understanding of computing systems to serve users' needs. Researchers in this field are focused on making universally usable, useful,

efficient, and appealing systems to support people in their wide range of activities. My approach is to balance the development of innovative technology that serves people's practical needs. I have combined my hardware and software skills throughout my career in HCI research, building various interactive electrical and mechanical systems that couple with software to provide an innovative user experience. Example systems that I have built include Pad++ (1994 software for zoomable user interfaces), KidPad (1997 software to support children collaboratively writing stories), PadPrints (1998 software to graphically show interactive web browsing histories), PhotoMesa (2001 software for end users to browse personal photos), Pocket PhotoMesa (2004 software for browsing of personal photos on a mobile device), DateLens (2002 software for end users to use their mobile devices to efficiently access their calendar information), LaunchTile (2005 "home screen" software for mobile devices to allow users to navigate apps in a zoomable environment), SpaceTree (2001 software for end users to efficiently browse very large hierarchies), ICDL (as described above), and StoryKit (a 2009 iPhone app for children to create stories).

11. My work on mobile devices includes software that I have publicly deployed. For example, DateLens, a calendar program for PDAs, was put on the Web in July 2002, and StoryKit, an iPhone app for children and their elders to create new books, was put in the iPhone App Store in August 2009. I am a named

inventor on U.S. patents relating to mobile devices and third party content, including U.S. Patent No. 9,778,810 (“Techniques to Modify Content and View Content on Mobile Devices”), U.S. Patent No. 11,061,524 (“Techniques to Modify Content and View Content on a Mobile Device”), and U.S. Patent No. 10,019,963 (“Systems and Methods for Adaptive Third Party Content”). I have also given invited talks on mobile topics, including “Designing for Usability” at the Mobile Marketing Association (New York, June 2007), “Mobile Technology Trends” (Knight Center for Specialized Journalism, September 2007), “Mobile Widget Design” (Widget Summit, October 2007), and “Next Generation Mobile UI” (Web 2.0 Expo, April 2008).

12. Pad++ included a custom web browser that I built from scratch and distributed as open source software at the Pad++ web site. That web browser was described in numerous publications including “Pad++: A Zoomable Graphical Interface for Exploring Alternate Interface Physics.” I implemented a rendering engine from scratch for that web browser which supported the version of HTML available at the time (HTML 1.0) as well as an embedded scripting language. That web browser included the ability to display embedded web pages created by the scripting language that could be zoomed along with the rest of the pages.

13. By 1998, my team had combined Pad++ with Netscape Navigator (a standard web browser of the time) to offer a graphical web history, visually

showing what pages a user had visited with an application we called “PadPrints.” We did this by implementing a web “proxy,” which was a standard way at the time to modify the built-in behavior of web browsers. Some proxies work by intercepting all web traffic coming from and going to a web browser. Once intercepted, the proxy can do whatever it wants with the traffic, caching it for better performance, simply passing the traffic through and monitoring it, modifying the data itself, or holding that connection and opening new connections. PadPrints’ proxy worked by monitoring the traffic and letting PadPrints know what the user was doing so PadPrints could display the web history.

14. At the International Children’s Digital Library (ICDL), I have since 2002 been the technical director responsible for the design and implementation of the web site, www.childrenslibrary.org (originally at www.icdlbooks.org). In particular, I have been closely involved in designing the user interface as well as the software architecture for the web site since its inception in 2002.

15. The ICDL GUI was designed for children to be able to construct searches consisting of combining multiple query terms including pre-defined metadata as well as open keywords. The GUI, as illustrated in the screenshot below included buttons around the periphery. When multiple buttons were pressed (or a keyword was entered), those terms would be ANDed together, sent to the server to perform the query, and the results were displayed in the center where the covers of

the books were displayed, eight at a time. Pressing the right arrow used AJAX web technology to dynamically retrieve and display the next 8 book covers from the server without having to reload the entire page. We switched from a similar-looking version of this interface to this AJAX-based approach in about 2006. The ICDL included URL parameters that were used to customize the page and to control navigation and search results.



Screenshot of Int'l Children's Digital Library,
<http://www.childrenslibrary.org/icdl/SimpleSearchCategory?ids=25&langid=1&pn=1&cnum=1&text=&lang=English&ilang=English> (screenshot taken Feb. 19, 2017).

16. Beginning in the mid-1990s, I have been responsible for the design and implementation of numerous other web sites in addition to the ICDL. For example, I designed and built my own professional web site when I was an Assistant Professor of Computer Science at the University of New Mexico in 1995 and have continued to design, write the code for, and update both that site (which I moved to the University of Maryland in 1998, currently at <http://www.cs.umd.edu/~bederson/>) as well as numerous project web sites, such as Pad++, <http://www.cs.umd.edu/hcil/pad++/>.

17. I started a new web-based project in 2009 to bring people together on a website to collaboratively translate text for children's books from one language to another. This resulted in numerous publications, including a 2011 paper that described a second generation of this work. In the numerous versions of this project, we used several web-based collaboration techniques, including by synchronous and asynchronous collaboration—allowing people to see the work of others on their own views of our website either immediately as others were doing the work (synchronously) or later after they had completed the work (asynchronously).

18. My work has been published extensively in more than 160 technical publications, and I have given about 100 invited talks, including 9 keynote lectures. I have won a number of awards including the Brian Shackel Award for

“outstanding contribution with international impact in the field of HCI” in 2007, and the Social Impact Award in 2010 from Association for Computing Machinery’s (“ACM”) Special Interest Group on Computer Human Interaction (“SIGCHI”). ACM is the primary international professional community of computer scientists, and SIGCHI is the primary international professional HCI community. I have been honored by both professional organizations. I am an “ACM Distinguished Scientist,” and I am a member of the “CHI Academy,” an honorary group of individuals who have made substantial contributions to the field of human-computer interaction. I have received two “Test of Time” awards from IEEE InfoVis for my 2001 and 2002 work on visualizing hierarchies, including those containing digital photos. I received the Janet Fabri Memorial Award for Outstanding Doctoral Dissertation for my Ph.D. work in robotics and computer vision.

19. I have appeared on radio shows numerous times to discuss issues relating to user interface design and people’s use and frustration with common technologies, web sites, and mobile devices. My work has been discussed and I have been quoted by mainstream media around the world over 120 times, including by the New York Times, the Wall Street Journal, the Washington Post, Newsweek, the Seattle Post-Intelligencer, the Independent, Le Monde, NPR’s All Things Considered, New Scientist Magazine, and MIT’s Technology Review.

20. I have designed, programmed, and publicly deployed dozens of user-facing software products that have cumulatively had millions of users. I am the co-inventor of 14 U.S. patents and 20 U.S. patent applications.

21. Since 2009, I have consulted as an expert witness, largely for patent infringement cases, for a range of clients.

III. COMPENSATION AND RELATIONSHIP WITH PARTIES

22. I am being compensated for my time. This compensation is not contingent upon my performance, the outcome of this matter, or any issues involved in or related to this matter.

23. I have no financial interest in Petitioner or any related parties. I have been informed that iQX Corp. (“iQX” or “Patent Owner”) owns the challenged patent. I have no financial interest in the outcome of this proceeding. I similarly have no financial interest in the challenged patent.

IV. MATERIALS CONSIDERED

24. I have reviewed and considered, in the preparation of this declaration, the following documents related to the challenged patent:

- the '924 patent (EX1001) and
- the prosecution file history of the '924 patent, Application No. 18/193,163 (EX1002).

25. I have also reviewed and understand various references as discussed herein, including the following:

- U.S. Patent No. 11,553,074 B1 to Brian Long et al. (“Long”) (EX1005 (Long));
- U.S. Patent Application Pub. No. 2012/0310752 to Gaddis (“Gaddis”) (EX1006);
- U.S. Patent No. 10,360,627 to Louie (“Louie”) (EX1007); and
- U.S. Application No. 15/986,569 (EX1013).

26. I understand that the paragraph immediately above lists references that form the basis for the grounds for invalidity set forth in the Petition for *Inter Partes* Review of the challenged patent.

27. I understand that, for purposes of determining whether a reference will qualify as prior art, the relevant date is the effective filing date of the claimed invention, which is determined claim by claim. I understand that no claim of the ’924 patent is entitled to an effective filing date earlier than September 27, 2018, the filing date of Provisional Application No. 62/737,315. Long, Louie, and Gaddis were each filed or have an effective filing date before September 27, 2018. EX1005 (Long), Cover; EX1006, Cover; EX1007, Cover.

28. Additionally, I am aware of prior and contemporary information relevant to the subject matter of the challenged patent and generally available to, and relied upon by, a person of ordinary skill in the art (a “POSITA”) to describe the state of the art as of the effective filing date of the challenged patent, including technical dictionaries, articles, and other technical reference materials (including,

for example, textbooks, manuals, technical papers, articles, and relevant technical standards), such as:

- B. Levine, “Led by TapCommerce founders, startup Attentive launches SMS/MMS marketing platform,” MarTech, dated Feb. 9, 2018, <https://martech.org/led-tapcommerce-founders-startup-attentive-launches-smsmms-marketing-platform/> (EX1008); and
- A. Ha, “TapCommerce’s founders are back with Attentive, a messaging startup that’s raised \$13M,” TechCrunch, dated Feb. 8, 2018, <https://techcrunch.com/2018/02/08/attentive-launch/> (EX1009);
- U.S. Patent No. 11,416,829 to Killoran, Jr. et al. (EX1010);
- U.S. Patent App. Pub. No. 2007/0150588 to Ghadialy et al. (EX1011);
- Shopify Help Center, “Abandoned checkouts” (Internet Archive capture dated Aug. 26, 2019) (EX1012);
- U.S. Application No. 15/986,569, filed May 22, 2018, to Brian Long et al. (EX1013);
- Yotpo Support, “Setting User Actions with Yotpo SMS & Email Texts as Rules in Segments” (Internet Archive capture dated Apr. 20, 2024) (EX1014);
- Twilio Experience, “Experience Helps Fans Have Live Events With Twilio,” (Internet Archive Capture dated Jan. 23, 2014) (EX1015);
- Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(1)(A)(iii) (EX1016);

- Fed. Commc'ns Commission, FCC 12-21, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 (2012) (EX1017);
- Mobile Marketing Association, U.S. Consumer Best Practices for Messaging Version 7.0 (Oct. 16, 2012) (EX1018);
- Mobile Marketing Association, Mobile Advertising Guidelines Version 5.0 (2011) (EX1019);
- U.S. Patent App. Pub. No. 2014/0024361 to Poon et al. (EX1020);
- U.S. Patent App. Pub. No. 2005/0278231 to Teeter (EX1021);
- Twilio Ruby Quickstart, "Twilio SMS and MMS Ruby Quickstart" (Internet Archive capture dated Jan. 23, 2014) (EX1022);
- U.S. Patent App. Pub. No. 2005/0228899 A1 to Wendkos et al. (EX1023);
- Payment Card Industry Security Standards Council, Information Supplement: Best Practices for Securing E-commerce (2017) (EX1024);
- U.S. Patent No. 9,298,844 to Graff et al. (EX1025);
- U.S. Patent Application Publication No. 2015/0100483 to Schoenberg (EX1026);
- U.S. Patent No. 5,960,411 to Hartman et al. (EX1027);
- iReachCompany, "Octane AI Launches Integration for Shopify, Ecommerce Conversational Commerce Platform, and New Partners" (May 1, 2018) (EX1028);

- Dan O’Shea, “Shopify Adds Facebook Messenger Direct Sales Channel” (Oct. 5, 2016) (EX1029);
- Gavin O’Malley, “Personalized Mobile Messaging: Game-Changer? Q&A With Attentive’s Brian Long” (Feb. 7, 2018) (EX1030);
- EmailChef, Marketing Glossary, <https://emailchef.com/email-marketing-glossary/> (EX1031);
- Katey Charles Communications, The Ultimate Email Marketing Glossary, <https://www.kateycharles.com/glossary#1479408991253-d4e0a31b-8ffd> (EX1032).

29. I reserve the right to supplement my opinions to address any information obtained, or positions taken, based on any new information that comes to light throughout this proceeding.

V. BASIS OF OPINIONS FORMED

A. Level of Ordinary Skill in the Art

30. It is my understanding that the challenged patent is to be interpreted based on how it would be understood by a POSITA at the time of the effective filing date of the application. It is my understanding that factors such as the education level of those working in the field, the sophistication of the technology, the types of problems encountered in the art, the prior art solutions to those problems, and the speed at which innovations are made may help establish the level of skill in the art.

31. I am familiar with the technology at issue and the state of the art at the effective filing date of the challenged patent, which, I understand, Patent Owner has represented is no earlier than September 27, 2018 for any claim.

32. In my opinion, a person having ordinary skill in the art at the time of the invention (“POSITA”) would have had 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.

33. I consider myself to have at least such ordinary skill in the art with respect to the subject matter of the challenged patent at the time of the effective filing date.

VI. THE ’924 PATENT

34. The ’924 patent is entitled “Secure Transactions Using Customized Webpages.” The ’924 patent includes claims 1-20, all of which are challenged in the Petition for *Inter Partes* Review.

A. Purported Invention of the '924 Patent

35. The '924 patent states that it relates to “techniques for performing transactions using dynamically generated customized webpages.” EX1001, 1:17-19.

36. According to the '924 patent specification, the prior art had two shortcomings. First, the popularity of online transactions “resulted in increased incidents of fraud and other criminal activity,” which “undermines people’s trust.” *Id.*, 1:24-28. Second, “many webpages or websites have largely static content that is presented or served to all visitors,” and this “one-size-fits-all approach” “often results in a cumbersome user experience.” *Id.*, 1:29-40. In other words, in the '924 patent the supposed problem is that websites show every visitor the same page, which it purports to address by showing each visitor a page assembled for that visitor.

37. The '924 patent describes a computer that “receives information specifying activation of a hosted field in a document associated with a third party (or potential client), where the information specifies a willingness to receive one or more messages from the computer and specifies a telephone number.” *Id.*, 3:39-44. In response, the computer “dynamically generates a customized second document that includes information about one or more transactions (such as one or more upcoming events) of interest to an individual (or potential subscriber

customer) associated with the telephone number.” *Id.*, 3:44-49. The computer then “sends a message to an address corresponding to the telephone number, where the message includes a link to the customized second document,” and, when it “receives information specifying activation of the link from an electronic device,” it “provides information specifying the customized second document to the electronic device for display.” *Id.*, 3:49-56.

38. One of the stated objectives of the ’924 patent is to “simplify the user experience, thereby increasing the likelihood that the individual (or potential subscriber customer) conducts the given transaction.” *Id.*, 3:65-4:1.

39. Figure 1 of the ’924 patent shows the components of the system: electronic devices 110 (such as a computer, a cellular telephone, or a tablet computer), a computer 112 (such as a cloud-based server), and a hosting computer 114, which communicate over a network 116 such as the Internet and, optionally, a cellular-telephone network 118. *Id.*, 4:40-52, Fig. 1. Computer 112 “may inject a hosted field into a document provided by hosting computer 114,” for example by providing the hosted field “for inclusion in a webpage associated with a third party (i.e., that is other than a provider of the communication technique).” *Id.*, 4:58-67. The hosted field allows a user “to indicate a willingness to receive one or more messages from computer 112 and that specifies a telephone number.” *Id.*, 5:3-7.

40. When the user activates the hosted field and provides a telephone number, that information reaches computer 112, which “may dynamically generate a customized second document (such as a webpage)” and “may send a message to an address corresponding to the telephone number, where the message includes a link to the customized second document.” *Id.*, 5:18-29. The message “may include a Short Message Service (SMS) message (which is sometimes referred to as a ‘text message’).” *Id.*, 5:29-31. When the user activates the link, computer 112 provides the customized second document to the user’s device for display. *Id.*, 5:32-44. Computer 112 may also provide “authentication information (such as an authentication cookie)” to the device “to authenticate completion of a given transaction.” *Id.*, 5:44-50.

41. Figure 2 of the ’924 patent, reproduced below, is a flow diagram of “method 200 for dynamically generating a customized document.” *Id.*, 8:23-26, Fig. 2. The computer receives information specifying activation of the hosted field (operation 210), dynamically generates the customized second document (operation 212), sends a message with a link to that document (operation 214), receives information specifying activation of the link (operation 216), and provides the customized second document to the electronic device for display (operation 218). *Id.*, 8:26-53.

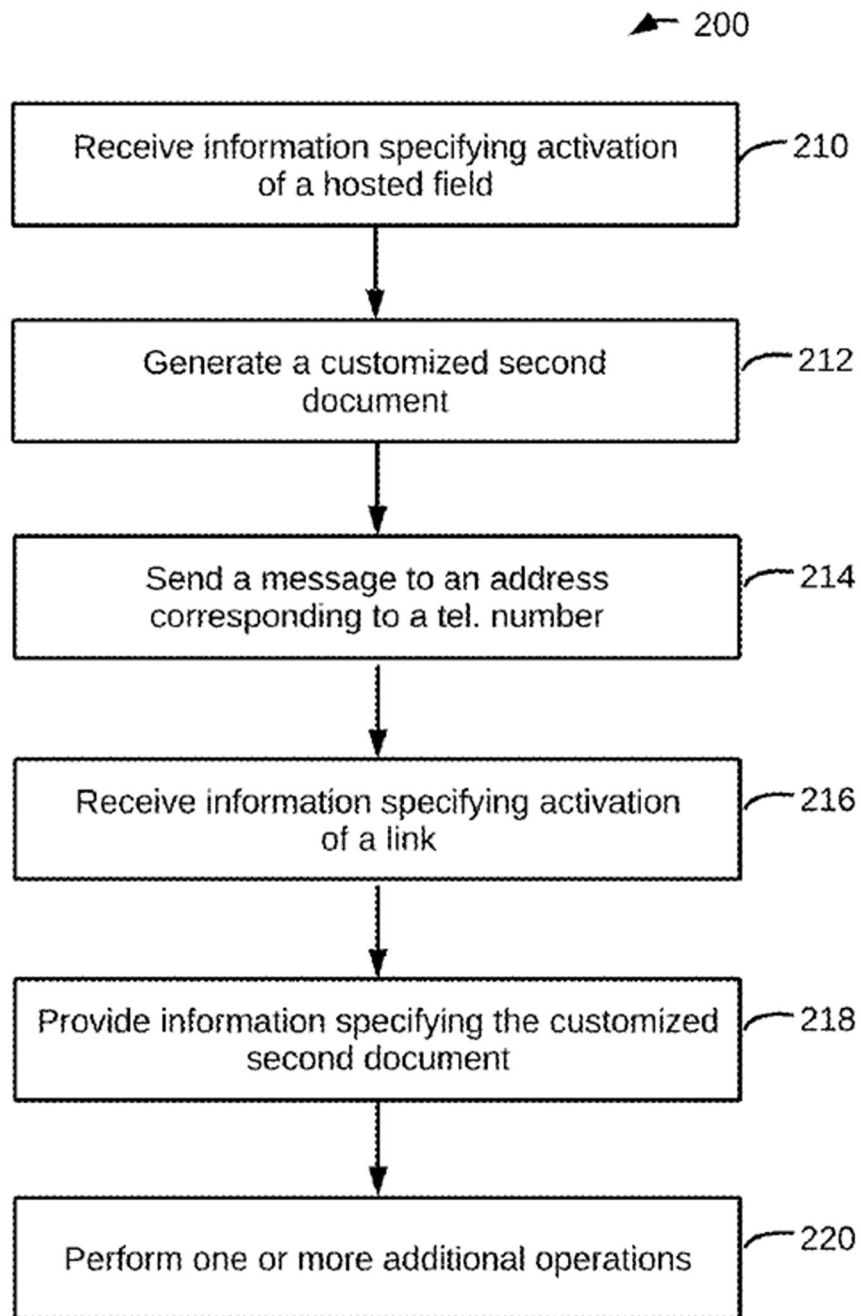


FIG. 2

The customized second document “may allow completion of a given transaction in the one or more transactions, such as purchasing one or more tickets to an upcoming event.” *Id.*, 5:55-58. Figure 3 shows the same sequence as

communications among computer 112, hosting computer 114, and electronic device 110-1, ending when the device “displays customized second document 322 on display 328.” *Id.*, 9:35-10:14, Fig. 3.

42. The specification describes the message as an SMS message, but states that “different communication channels may be used in other embodiments, e.g., email, Enhanced Messaging Service (EMS), and/or Multimedia Messaging Service (MMS).” *Id.*, 10:27-31. In other words, the ’924 patent itself states that it is agnostic as to the choice of messaging channel, which signals to a POSITA that this is not what the patent regards as any sort of technical contribution.

43. The specification explains that the customized webpage “may be created de novo for each subscriber customer or individual,” and that “[a] given subscriber customer cannot hit their webpage without a specific link that is provided to the given subscriber customer.” *Id.*, 10:36-42. If the link is shared with a second individual, that individual “may browse content customized for the first individual but will be prohibited from accessing a profile of the first individual and/or executing a transaction unless the second individual subscribers [sic] and provides his/her telephone number.” *Id.*, 10:45-51.

44. Figures 4 through 7 describe a commercial implementation that the specification calls “Amplify,” in which the hosted field is injected “into client web-purchase forms generated by the third-party API platform 402,” and a message is

sent with “a link to purchase tickets or view a customized webpage.” *Id.*, 12:7-13, 12:33-42, 12:57-65.

45. I refer now to the claims of the '924 patent. The '924 patent has 20 claims. Claims 1, 8, and 15 are independent and are directed to a computer-implemented method, a system, and a non-transitory computer-readable storage medium, respectively. The claims, and the labels I use for the elements of the independent claims, are reproduced below. EX1001, 20:45-22:63.

Claim	Claim Language
1[pre]	A computer-implemented method comprising:
1[a]	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;
1[b]	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,
1[c]	wherein the at least one customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber;
1[d]	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; and
1[e]	causing transmission of the generated third party message to the service subscriber.

Claim	Claim Language
2	The computer-implemented method of claim 1, wherein 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.
3	The computer-implemented method of claim 1, wherein the third party message is associated with a third party ticket provider, a third party service provider, or a third party event provider.
4	The computer-implemented method of claim 1, wherein 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.
5	The computer-implemented method of claim 1, wherein the at least one customized actionable item comprises a secure link to perform the e-commerce transaction for purchasing tickets, merchandise, or products.
6	The computer-implemented method of claim 1, wherein the authentication information comprises an authentication cookie configured to be stored on an electronic device associated with the service subscriber.
7	The computer-implemented method of claim 1, wherein the third party message comprises a Short Message Service (SMS) message or a Multimedia Message Service (MMS) message.
8[pre]	A system comprising:
8[a]	a processor; and

Claim	Claim Language
8[b]	memory configured to store program instructions, wherein, when executed by the processor, the program instructions cause the processor to perform operations comprising:
8[c]	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;
8[d]	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,
8[e]	wherein the at least one customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber;
8[f]	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; and
8[g]	causing transmission of the generated third party message to the service subscriber.
9	The system of claim 8, wherein 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.
10	The system of claim 8, wherein the third party message is associated with a third party ticket provider, a third party service provider, or a third party event provider.

Claim	Claim Language
11	The system of claim 8, wherein 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.
12	The system of claim 8, wherein the at least one customized actionable item comprises a secure link to perform the e-commerce transaction for purchasing tickets, merchandise, or products.
13	The system of claim 8, wherein the authentication information comprises an authentication cookie configured to be stored on an electronic device associated with the service subscriber.
14	The system of claim 8, wherein the third party message comprises a Short Message Service (SMS) message or a Multimedia Message Service (MMS) message.
15[pre]	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:
15[a]	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;
15[b]	activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction to purchase tickets, merchandise, or products or view the one or more customized webpages depicting information about the tickets, merchandise, or products, the activating comprising generation of secure access information for performing the e-commerce transaction,

Claim	Claim Language
15[c]	wherein the at least one customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber;
15[d]	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; and
15[e]	causing transmission of the generated third party message to the service subscriber.
16	The non-transitory computer-readable storage medium of claim 15, wherein the third party message is associated with a third party ticket provider, a third party service provider, or a third party event provider.
17	The non-transitory computer-readable storage medium of claim 15, wherein 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.
18	The non-transitory computer-readable storage medium of claim 15, wherein the at least one customized actionable item comprises a secure link to perform the e-commerce transaction for purchasing tickets, merchandise, or products.
19	The non-transitory computer-readable storage medium of claim 15, wherein the authentication information comprises an authentication cookie configured to be stored on an electronic device associated with the service subscriber.
20	The non-transitory computer-readable storage medium of claim 15, wherein the third party message comprises a Short Message Service (SMS) message or a Multimedia Message Service (MMS) message.

46. I use the same element labels as the Petition. Claims 8 and 15 recite the same five operations as elements 1[a] through 1[e]; elements 8[c]-8[g] and 15[a]-15[e] correspond to elements 1[a]-1[e], respectively. EX1001, 20:45-22:63. Claim 15 differs in one respect. Element 15[b] additionally recites 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,” which is the subject matter that claim 2 adds to claim 1. Claim 15 accordingly has five dependent claims where claim 1 has six.

47. The dependent claims add features such as webpages for viewing or purchasing tickets, merchandise, or products (claims 2, 9) (which is recited in limitation 15[b] rather than in a dependent claim of claim 15); third party messages associated with a third party ticket, service, or event provider (claim 3, 10, 16) or including the link (claim 4, 11, 17); a secure link (claim 5, 12, 18); an authentication cookie stored on the user’s device (claim 6, 13, 19); and third party SMS and MMS messages (claim 7, 14, 20). EX1001, 20:66-21:28, 21:53-22:12, 22:40-63.

48. As I explain in Section IX.A *infra*, each of these functions was known before the ’924 patent, and in Sections IX.C and IX.D, I explain how the prior art renders the claims obvious.

B. Prosecution History

49. I have reviewed the prosecution history of the '924 patent. I have been informed by counsel and understand that statements made during prosecution of a patent may influence the meaning of terms in the claim of that patent, as well as terms in other claims in the same patent family.

50. The '924 patent issued from Application No. 18/193,163 ("the '163 application"), filed on March 30, 2023 as a continuation of Application No. 17/279,188. EX1001, 1:5-13; EX1002, 240.

51. The claims of the '163 application map to the issued claims as follows. Application claim 25 issued as claim 1, claims 26-31 issued as claims 2-7, claim 32 issued as claim 8, claims 33-38 issued as claims 9-14, claim 39 issued as claim 15, and claims 40-44 issued as claims 16-20. EX1002, 231-35; EX1001, claims 1-20.

52. On November 9, 2023, the Examiner issued a non-final Office Action rejecting claims 2-11, 14-15, and 22-23 of the '163 application as anticipated by U.S. Patent App. Pub. No. 2017/0295414 ("Murray"), allowing claims 25-31, and objecting to claim 24 but noting it would be allowable if rewritten in independent form. EX1002, 184, 188. At the time, the applicant had filed two preliminary amendments, the first on June 13, 2023 and the second on September 28, 2023. *Id.* at 149, 174. The second cancelled claims 1 and 16-21 and newly added claims 22-

31, with claim 25 presented as an independent claim. *Id.* at 167-73. In that amendment the applicant stated that “No new subject matter has been added” and that “Support for the amendments and new claims can be found throughout the specification as filed, at least at paragraphs [068]-[092] and FIGS. 4-6.” *Id.* at 173. Claim 25, as presented in that preliminary amendment, already recited every limitation of issued claim 1, including “configuring a service subscriber associated with a telephone number,” “the activating comprising generation of secure access information,” and the “customized actionable item correspond[ing] to prior actions associated with one or more prior transactions performed by the service subscriber.” *Id.* at 171. Independent claim 2 had required, among other limitations, “providing, to a third party, a subscriber customer identifier” and “generating . . . a customized webpage that includes . . . a secure transaction opportunity correspond[ing] to an interest of the subscriber.” *Id.* at 167.

53. The Examiner reasoned that Murray taught the providing of a subscriber customer identifier via “programmable code” within an online interactive media file that “pull[s] in all of the functional assets from [a] third party web service provider.” *Id.* at 185-86. The Examiner also reasoned that Murray taught the generation of a customized webpage that includes a secure transaction opportunity corresponding to an interest of the subscriber via Murray’s interactive media player allowing “the end user device 1509 [to] then interact with interactive

media file, as though it is a self-contained software application, without leaving the current webpage.” *Id.* at 186.

54. The Examiner addressed several dependent claims individually. For claim 3, the Examiner found the “authentication cookie configured to be stored on an electronic device associated with the subscriber and customized webpage” limitation disclosed by Murray’s hypermedia link icon embedding functionality—specifically, that “when a client enters the cloud suite, they are able to . . . embed hypermedia link icons by clicking on elements they see and when a hypermedia link icon is embedded, a user is able to populate it.” *Id.* at 186. For claim 4, the Examiner found that Murray’s interactive media player, wherein “a user can click an item seen within the primary multimedia content . . . and perform a complete transaction,” anticipated the limitation for “the customized webpage facilitat[ing] completion of at least one of the transaction opportunities.” *Id.* at 186-87.

55. In response to the Examiner’s non-final rejection, the applicant filed an amendment on November 16, 2023. The applicant cancelled all of the rejected claims and claim 24, and presented new claims 32-44. *Id.* at 230-35, 238. New independent claims 32 and 39 recited the same operations as already-allowed claim 25, in system and non-transitory computer-readable storage medium form respectively. *Id.* at 232-35 (claim 32 at 232, claim 39 at 234). The applicant stated that it had “cancelled claims 1-24 and added new claims that include the allowable

subject matter” in order “[t]o expedite issuance of the allowed claims,” and that it did so “[w]ithout acquiescing or otherwise agreeing with the rejections of record.” *Id.* at 236. The applicant further stated that claims 1-24 were “cancelled without prejudice or disclaimer to the subject matter therein.” *Id.* The applicant advanced no argument distinguishing Murray on the merits. *Id.*

56. The dependent claims were also changed. *Id.* at 231-35. The only substantive amendment was to claim 30, the authentication cookie claim, which the applicant changed from a cookie “stored on an electronic device associated with the subscriber” to one “stored on an electronic device associated with the service subscriber.” *Id.* at 232. New claims 37 and 43 recited that same limitation. *Id.* at 233, 235.

57. The Examiner then allowed claims 25-44 in a Notice of Allowance mailed December 7, 2023. *Id.* at 240-46. The reasons for allowance stated that “the prior art of record either singularly or in proper combination fails to teach” the recited operations, which the Examiner quoted as 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, activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction, generating a third party message associated with those

webpages and including that actionable item, and causing transmission of the message to the service subscriber. *Id.* at 245. The Examiner identified claims 25, 32, and 39 as the claims to which that reasoning applied, and allowed “[a]ll dependent claims ... under same reasons set forth above.” *Id.* at 246.

58. The Examiner used the same recitation twice. The statement of allowable subject matter in the November 9, 2023 Office Action and the statement of reasons for allowance in the Notice of Allowance begin with word-for-word identical text. *See id.* at 188, 245. The Office Action version ends after “activating one or more customized webpages including at least one customized actionable item for performing an e-commerce transaction,” while the Notice of Allowance version continues through the generating and transmission steps. *Id.* at 188, 245. Neither version recites the limitation that “the activating compris[es] generation of secure access information for performing the e-commerce transaction,” and neither recites the limitation that the “customized actionable item corresponds to prior actions associated with one or more prior transactions performed by the service subscriber.” *Id.*

59. Long, Louie, and Gaddis were not cited by the applicant or the Examiner during prosecution of the '924 patent. EX1001, References Cited.

VII. CLAIM CONSTRUCTION

A. Legal Standard for Claim Construction

60. It is my understanding that in an *inter partes* review proceeding, a claim of a patent is construed using the same claim construction standard that would be used to construe the claim in a civil action, including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

61. I am not a patent attorney and my opinions are limited to what I believe a POSITA would have understood the meaning of certain claim terms to be, based on the patent specifications and prosecution histories.

62. A POSITA would have no difficulty applying the plain and ordinary meanings of the terms used in the claims.

63. For purposes of this declaration, I have interpreted the terms of claims 1-20 of the '924 patent according to their plain and ordinary meaning.

VIII. OBVIOUSNESS STANDARD

64. It is my understanding that obviousness is a question of law based on underlying factual issues including (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claim, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations such as commercial success, long-felt but unresolved needs, failure of others, etc.

65. I understand that for a single reference or a combination of references to render obvious the claimed invention, a POSITA must have been able to arrive at the claim by altering or combining the applied references.

66. I understand that an obviousness evaluation can be based on a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references is simple common sense. I further understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

67. I understand that if a technique has been used to improve one device or product, and a POSITA would recognize that it would improve similar devices or products in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

68. I also understand that practical and common sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a POSITA looking to overcome a problem will often be able to fit together the teaching of multiple references. I understand that obviousness analysis therefore takes into

account the inferences and creative steps that a POSITA would employ under the circumstances.

69. I understand that a particular combination may be proven obvious merely by showing that it was obvious to try the combination. For example, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a POSITA has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

70. I also understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a work is available in one field of endeavor, design incentives and other market forces can prompt variation of it, either in the same field or a different one. If a POSITA can implement a predictable variation, the patent claims are likely obvious.

71. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a POSITA, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor before the effective filing date of the claimed invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

72. I understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art. In addition, a reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art, including nonpreferred embodiments. Disclosed examples and preferred embodiments do not teach away from a broader disclosure or nonpreferred embodiments.

73. I understand that a reference may be relied on in an obviousness analysis only if it is analogous art to the claimed invention. I understand that a reference is analogous art if it is from the same field of endeavor as the claimed invention, regardless of the problem it addresses, or, if it is not, if it is reasonably pertinent to the particular problem with which the inventor was involved.

74. I understand that secondary indicia of non-obviousness may include (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) commercial success of processes covered by the patent; (3) unexpected results achieved by the invention; (4) praise of the invention by others skilled in the art; (5) taking of licenses under the patent by others; (6) deliberate copying of the invention; (7) failure of others to find a solution to the long felt need; and (8) skepticism by experts.

75. I also understand that there must be a relationship between any such secondary considerations and the invention. I further understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

76. In sum, my understanding is that prior art teachings are properly combined or modified where a POSITA having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claim. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor before the effective filing date of the claimed invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

IX. ANALYSIS OF THE TECHNICAL BASIS UNDERLYING THE GROUNDS OF REJECTION SET FORTH IN THE PETITION FOR *INTER PARTES* REVIEW

A. State of the Art

77. The '924 patent states that its disclosure relates to “security and access control for cellular handheld devices” and to “techniques for performing transactions using dynamically generated customized webpages.” EX1001, 1:17-36.

78. As described further below, the challenged claims recite configuring a service subscriber associated with a telephone number in response to the subscriber previously providing authentication information, activating a customized webpage with a customizable action item for performing an e-commerce transaction wherein the customizable action item corresponds to the subscriber's prior transactions, generating a third party message associated with the customized webpage, and causing transmission of the third party message; the dependent claims add an SMS message format, an authentication cookie, secure links, and associating the third party and actionable item with tickets, services, merchandise, products, and events. EX1001, 20:45-22:63. In the subsections below I describe what the documents I reviewed show about each of these subjects before the '924 patent.

79. I address the state of the art as of September 27, 2018. I understand that Petitioner treats this date as the earliest date to which any challenged claim could be entitled. For each document below I note its date.

80. As I explain below, each of these functions was known, and was described in published patents, standards, and industry documentation, before the '924 patent.

1. Configuring Subscriptions Associated With Customers' Phone Numbers and SMS-Based Marketing

81. Subscribing a customer to receive SMS-based marketing content was a well-known practice long before the '924 patent.

82. For example, the prior art discloses users providing permission and preferences regarding receiving SMS-based messages from e-commerce retailers. Indeed, as early as 2007, a prior art patent application US 2007/0150588 to Ghadially (EX1011) described consumers subscribing to receive alerts on topics of interest and choosing “a desired delivery option, such as via E-Mail, IM, RSS, SMS, or a Web portal,” and being given “a set of options to allow the user to opt out of receiving further messages.” EX1011 (Ghadially), ¶¶20, 23-24.

83. Likewise, as of 2012, six years before the priority date of the '924 patent, U.S. Patent Application Pub. No. 2012/0310752 A1 to Gaddis recognized that e-commerce and online marketing “ha[d] exploded over the past few years becoming a multi-billion dollar industry,” in which “[a]dvertisements can be sent directly to potential buyers (i.e. Users) via email, SMS-text, Instant Messaging, Tweets, Facebook posts, and other emerging formats.” EX1006 (Gaddis), ¶3. Gaddis describes users being sent offers only if they “have previously indicated that they would be interested in receiving correspondence from the merchant,” noting that a service provider sending an offer via text message involves the user providing “a cell phone number.” EX1006, ¶¶48, 54.

84. The same practice was built into commercial platforms on which merchants ran their e-commerce stores. For instance, Shopify system’s checkout recorded “[w]hether the customer would like to receive email updates from the

shop,” as indicated by a checkbox at checkout, along with “[t]he customer’s phone number for receiving SMS notifications.” EX1012, 2, 5. And text-message marketing platforms like Yotpo tracked which customers had “confirmed their subscription to receive marketing messages.” EX1014, 1. Twilio, another text-message marketing platform, allowed merchants to market their recurring, subscription-based services by having consumers “sign up [and] include their phone number and opt in consent.” EX1015, 4

85. A POSITA would know that these opt-in practices were not merely industry standard, they were regulated into existence by the federal government well before the priority date of the '924 patent. *See, e.g.*, EX1005 (Long), 6:53-57. 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”), which I rely on as prior art below, for example, cites the Telephone Consumer Protection Act of 1991 (“TCPA”), which prohibits sending autodialed calls to a wireless number without the recipient's prior express consent. 47 U.S.C. § 227(b)(1)(A)(iii) (EX1016 (TCPA)). In February 2012, the FCC adopted rules requiring “prior express written consent” before a marketer may send autodialed telemarketing calls or text messages to a wireless number. EX1017 (FCC 2012 TCPA ORDER).

86. Consistent with those regulations, Long discloses sending messages only after customer opt-in to ensure “compliance with the Telephone Consumer Protection Act (‘TCPA’) and the regulations by trade associations representing the wireless communication industry (e.g., CTIA).” EX1005, 6:53-57, 15:36-38. Other trade associations, like the Mobile Marketing Associations developed and published standards, guidelines, and best practices references regarding the implementation of opt-in and consent forms as a prerequisite to transmitting marketing content to mobile devices, years before the ’924 patent’s priority date. EX1018, 8 (“Content providers must obtain opt-in approval from subscribers before sending them any SMS or MMS messages or other content from a short code.”); *see also* EX1019, 11-12. A POSITA would have understood that obtaining a consumer’s consent, together with the consumer’s phone number, before sending marketing text messages to that number was a routine practice and both an established industry standard and a regulated government requirement.

2. User Authentication, Secure Links, and Cookies

87. Before the ’924 patent, it was likewise well known to configure a user’s subscription once the system determined that the customer had provided authentication information. The prior art shows that such systems confirmed, before granting access to a resource specific to a given subscriber, that the person holding the device or telephone number was that subscriber, and did so using

whatever identifier the system already had on hand—including by collecting a customer’s phone number, contact information, or security credentials; using cookies to recognize the customer; texting the customer a confirmation link; and sending encrypted, secure links.

88. U.S. Patent Application Pub. No. 2014/0024361 to Poon discusses entering “a specific code to the device, which indicates that the device and its embedded SIM are to be provisioned to provide all of the services that the subscriber has subscribed to,” and that such specific code “may also include security credentials that can be used to verify that the subscriber in question is allowed to use the device and SIM in question.” EX1020, ¶¶69, 72.

89. Twilio likewise described the collection and acting upon of authentication information as early as 2014, providing an “identity verification system” that “texts a confirmation link” to a phone number provided by a consumer. EX1015, 4. “Once the [consumer] taps that link, they get access.” EX1015, 4.

90. Another prior art patent application, U.S. Patent Application Pub. No. 2005/0278231 to Teeter, also discusses such authentication information collection, noting that a customer’s contact information can be collected from the e-commerce “website’s checkout or site registration e-mail address collection form field,” “a cookie placed from a prior site visit,” “from a prior site visit by a previously

registered consumer that logged in during the current session,” or “from a data collection panel presented during the session via a pop up window or hidden <div> element block hosted by either the e-commerce website or a 3rd party application service provider (ASP).” EX1021, ¶13.

a. Cookies

91. Using cookies was a well-known technique of collecting authentication information. Teeter, as explained above, offered such a technique, describing a customer’s contact information being collected from “a cookie placed from a prior site visit.” EX1021, ¶13. Ghadialy likewise explains that a system “can use a set of HTTP cookies to track the identity of the user,” on sign-up pages on a merchant’s website. EX1011, ¶21.

92. Similarly, Gaddis, which I address as prior art in my Ground 1 and Ground 2 analysis below, explains that using cookies to collect authentication information was routine. Gaddis describes its “User” as someone “whose identity has been previously verified by the Offer Provider,” and explains that such verification may occur where the User “is verified by cookies or other method well known by the skilled artisan.” EX1006, ¶¶37, 61.

93. Twilio also describes user authentication through the use of cookies: “Just like in web applications, a cookie is a small file that your application can store on Twilio’s servers to keep track of information, such as a username or

account. For Twilio SMS, cookies are scoped to the ‘conversation’ between two parties -- you can have a unique cookie for each To/From phone number pair.”

EX1022, 11. Twilio even explained the utility of cookies in this regard, emphasizing that doing so “keep[s] ‘statefulness’ between separate requests from the same browser. Similarly, SMS messages are independent communications between two parties, so Twilio allows you to tie them together as a logical session via cookies.” EX1022, 11.

b. Secure Links

94. The sending of secure links was also well known and frequently in use before the ’924 patent issued. For example, Gaddis describes the sending of email links or SMS links that are “encrypted before sending to User and decrypted by” the offer provider. EX1006, ¶34. Similarly, U.S. Patent Application Publication No. 2005/0228899 A1 to Wendkos describes “encrypted URL[s] which can only be viewed by the recipient.” EX1023, ¶37.

95. U.S. Patent No. 11,416,829, which was filed on July 13, 2016 as Appl. No. 15/209,338, to Killoran Jr. et al., likewise describes sending secure links to consumers via SMS. Killoran describes a technique where “[t]okens may be encrypted or plain text strings which contain information to perform a transaction when sent to the e-commerce system 140,” and that “[a] token may be one or multiple encrypted strings, files, passwords, cyphers, plain text or other data which

may contain information used to perform or authenticate a transaction.” EX1010 (Killoran), 7:48-52. Killoran’s system generates both a “short lookup token” and a “long token,” where the short token “may be required or otherwise needed to access the information in the long token index,” *Id.*, 18:58-62, generates “a short URL that corresponds to the short token and the long token,” and then “generates an SMS offer or social media post offer message with the short URL Link” and sends it to the customer’s device, *Id.*, 31:49-55. Killoran adopted that approach because despite the growth of SMS payment methods, there were known security problems—saying SMS could be “easily hacked”—that needed to be addressed. *Id.*, 1:62-63.

96. The e-commerce industry widely recognized the importance of maintaining security around sensitive consumer information. Not only was the sending of secure links to personalized web pages common generally, but so was the sending of secure links in connection with e-commerce transactions. In 2017, the Payment Card Industry Security Standards Council, a trade association that develops standards for the payment card industry, published a standard titled “Best Practices for Securing E-commerce,” in which “encrypted transmission” of “cardholder data . . . across open, public networks” was regarded as paramount. EX1024, 31.

97. Thus, the collection and response to authentication information—including that comprising cookies—was standard practice long before the '924 patent's priority date, as was the provisioning of secure links.

3. Customized Web Pages

98. Sending a consumer a link that directs to a webpage that is unique to that consumer was a standard technique.

99. Web pages are accessed via URLs, and a URL can include more components than just the address of a web page. URLs can include parameters, typically after a “?” character, that the web server reads when the request arrives. *See, e.g.*, EX1006, ¶¶57, 64 (“?deal=123”); EX1012, 1. These parameters can identify the recipient, such that the server knows the identity of who clicked on the URL and subsequently review stored information related to that recipient and generate a unique page for that recipient accordingly, as opposed to returning the same page for every recipient. *See, e.g.*, EX1006, ¶¶57-59. U.S. Patent No. 9,298,844 to Graff described a “unique URL referenc[ing] a web page that will dynamically route the web browser to a specific webpage based on the results of the queries logged by the web servers at the time the unique URL is accessed.” EX1025, 3:3-8. The server can also redirect the browser to another address, and it can place a cookie on the browser so that it recognizes the same visitor on later requests. *See, e.g.*, EX1006, ¶59; EX1025, 3:3-8; EX1011, ¶21.

100. These are well known, basic web programming techniques. *See, e.g.*, EX1006, ¶¶57-58. In 1998, my team built a web proxy that monitored the requests a browser sent and the pages it received. In 2001, my team used personalized URLs in the International Children’s Digital Library. I have used all these techniques in the web sites I have built since the early 2000s. *See supra* Section II.

101. Gaddis described this precise functionality in 2012. Its link incorporates “parameters passed in URL,” including “the User identification (encrypted),” so that clicking the link directs a recipient to a webpage “created specifically for the merchant’s advertisement and the User.” EX1006, ¶¶57, 59. Gaddis treats the page-building as routine, stating that the service provider can create a webpage specific to each user “by methods well known in the art.” EX1006, ¶58.

102. Others described the same arrangement specifically applied for use in a text message-based system. Schoenberg, published in 2015, describes sending a text message with a URL “personalized to uniquely identify the customer,” that directs the user to a mobile web page “without the customer logging in.” EX1026, ¶7. Graff described a system in 2016 in which “[e]ach intended message recipient will receive a different unique URL,” and the unique URL “references a web page that will dynamically route the web browser to a specific webpage” based on what the server learns upon activation of the link. EX1025, 2:57-62, 3:3-8.

103. The generation of web pages customized to individual consumers was thus known and practiced often before the '924 patent.

4. Interactive Elements that Enable Purchasing of Products Tailored to the Consumer's Interests

104. The fields of e-commerce and online marketing were also rife with examples of customized webpages including interactive elements that allowed consumers to make purchases.

105. Since as early as 1999, for example, Amazon utilized a shopping functionality for users to purchase a product online by “display[ing] an indication of an action (e.g., a single action such as clicking a mouse button) that a purchaser is to perform to order the identified item,” wherein “[i]n response to the indicated action being performed, the client system sends to a server system the provided identifier and a request to order the identified item.” EX1027, 2:51-3:7.

Unsurprisingly, Gaddis reflects that the state of the art in 2012 included buyers “input[ting] . . . their personal and billing information with each website visit wherein a purchase is made.” EX1006, ¶3.

106. Teeter describes this functionality as well, in the context of an abandoned cart e-commerce flow. When consumers are shopping online and add products to their online shopping carts, they often abandon their shopping journey before making any purchases. Teeter's method saves the shopping cart and the consumer's information during the online shopping journey and, if the shopping

cart is abandoned, “automatically prompt[s] the abandoned shopper with an e-mail message or other electronic communication to reinitiate the checkout process from a hyperlink in the e-mail message or other form of communication.” EX1021, ¶6.

107. This functionality was being used in real-world applications as well. Shopify gave online stores “the ability to directly message customers when they abandon their shopping carts,” and presented a way for consumers to be “presented with a ‘Shop Now’ option to view a product catalog, and [to] complete a purchase using Shopify’s checkout tools.” EX1028, 2; EX1029, 1.

108. Moreover, it was common for the products made available for purchase in these interactive elements to be specifically presented to the consumer based on the consumer’s past purchases. The Attentive system provided a “personalized messaging platform” that used “behavioral data (like past purchases, for example)” to “remind someone that it’s time to restock one of their favorite products, or recover an abandoned shopping cart.” EX1030, 2.

109. Similarly, Poon described a “recommendation engine . . . for creating real-time contextual offers.” EX1020, ¶139. This recommendation engine “analyze[d] information collected from . . . campaigns . . . by data mining” in order to “make offers that are most relevant” to a particular subscriber. EX1020, ¶139. The result was that a “recommendation could be made with respect to a number of

factors of contextual assessment, such as time in contract, loyalty status, purchase history, value of customer, and data and time usage.” EX1020, ¶139.

110. Thus, many practitioners in the art before the '924 patent described and engaged in including interactive elements in customized web pages that facilitated the purchasing of products—particularly products that were specifically recommended to a particular consumer based on that consumer’s previously made purchases.

B. Specific References that Render the Claims Obvious

1. Secondary Considerations

111. I am unaware of any secondary considerations that would render the claims of the challenged patent non-obvious.

C. Ground 1: Claims 1-20 Are Rendered Obvious by Long in View of Gaddis and the General Knowledge of a POSITA

112. In my opinion, claims 1-20 of the '924 patent are rendered obvious by Long in view of Gaddis and the general knowledge of a POSITA. Long in view of Gaddis and the general knowledge of a POSITA discloses or renders obvious each element of independent claims 1, 8, and 15 and of dependent claims 2-7, 9-14, and 16-20.

1. U.S. Patent No. 11,553,074 to Long

113. 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”), was filed on October 7, 2021, and issued on January 10, 2023.

EX1005 (Long), Cover. Long is a continuation of U.S. Application No.

15/986,569, filed May 22, 2018, which claims priority to U.S. Provisional

Application No. 62/511,413, filed May 26, 2017. *Id.*, Cover, 1:5-16.

114. I have reviewed U.S. Application No. 15/986,569 (EX1013), and each disclosure of Long on which I rely below also appears in that application. I have also compared the two specifications. Other than the cross-reference to related applications, the specification of Long is word for word identical to the specification of the ’569 application. Everything Long’s specification discloses, the ’569 application discloses in the same words.

115. I understand that Long is therefore prior art to the ’924 patent. Long was not cited by the applicant or the Examiner during prosecution of the ’924 patent. EX1001, References Cited.

116. I understand that the continuity between Long and Application No. 15/986,569 is relevant to its status as prior art. Long issued from Application No. 17/496,590, which was filed on October 7, 2021. EX1005 (Long), Cover. On October 8, 2021, counsel for the applicant filed an Express Abandonment in Application No. 15/986,569. EX1013, 623. That paper identifies Application No. 15/986,569, filed May 22, 2018, with Brian Long as the first named inventor, and selects the option for “Express Abandonment in Favor of a Continuing

Application,” by which the applicant requested that the application “be expressly abandoned as of the filing date accorded the continuing application filed previously or herewith.” *Id.* Long’s cover page reflects the resulting abandonment, reciting a “[c]ontinuation of application No. 15/986,569, filed on May 22, 2018, now abandoned.” EX1005 (Long), Cover. Because Application No. 17/496,590 was filed on October 7, 2021, and the express abandonment of Application No. 15/986,569 was not filed until October 8, 2021, the two applications were co-pending, and the express abandonment was made in favor of the continuing application that had been “filed previously.”

117. Counsel has advised me that, a patent is prior art if it names another inventor and was effectively filed before the effective filing date of the claimed invention. Further, counsel has advised me that such a patent is deemed effectively filed, as to any subject matter described in it, as of the filing date of the earliest application to which the patent is entitled to claim a benefit as to that subject matter. Counsel has further advised me that entitlement to benefit of an earlier application requires, among other things, that the later application be filed before the patenting or abandonment of the earlier application. Applying that framework, and because Application No. 17/496,590 was filed while Application No. 15/986,569 remained pending as described above, it is my understanding that Long

is deemed effectively filed no later than May 22, 2018 as to the subject matter described in Application No. 15/986,569.

118. I have compared the two specifications, and each disclosure of Long on which I rely below is described in Application No. 15/986,569. EX1013; EX1013, 22-61, 80, 93-122. Long also claims the benefit of Provisional Application No. 62/511,413, filed May 26, 2017, which I have not reviewed for purposes of determining whether Long is prior art. EX1005 (Long), Cover. May 22, 2018, the date of the '569 application filing including the disclosures on which I rely below, precedes September 27, 2018, the earliest date to which the '924 patent claims priority. EX1001, 1:5-13. I therefore understand Long is prior art to the '924 patent.

119. Long also names different inventors and a different owner than the '924 patent. Long names Brian Long and six co-inventors and is assigned to Attentive Mobile Inc. of New York, New York. EX1005 (Long), Cover. The '924 patent names Sacha Spindler, Andrew Lewin, and Aidan Wright as inventors and is assigned to iQX Corp. of Carson City, Nevada. EX1001, Cover. I am not aware of any evidence that the subject matter of Long was obtained from the named inventor of the '924 patent, that it was publicly disclosed by that inventor before Long was effectively filed, or that Long and the '924 patent were owned by or subject to an obligation of assignment to the same person.

120. Long is assigned to Attentive Mobile Inc., a New York-based text-message marketing company. EX1005 (Long), Cover. Contemporaneous materials describe Attentive’s offering as aimed “at ecommerce and retail brands,” as supporting “SMS and MMS messages” used for “targeted promotions, retargeting, customer service, transactions (i.e., purchases made via text messaging) or retention,” and as providing a “two-tap” enrollment path. EX1008, 1; EX1009, 3. Those materials also report a \$13 million Series A financing announced in February 2018. EX1009, 1.

121. Long describes a “click-to-text” platform that allows a consumer to subscribe to an online vendor’s text messages and complete purchases from that vendor using text messages and links to checkout pages. EX1005 (Long), 1:20-25, 2:18-32. The problem in the art that Long addresses is the “time-consuming and burdensome process” when a mobile device user “often pauses its previous activities (e.g., viewing a website, reading an email)” to navigate a vendor’s application or website, which “results in many users leaving the purchase before the transaction is completed.” *Id.*, 1:25-37.

122. Figure 1 of Long depicts three entities that make up its platform: click-to-text server 100, client server 130, and user mobile device 150. *Id.*, Fig. 1.

123. Click-to-text server 100 communicates with client server 130 and user mobile device 150 via a network and includes at least one processor 101 and at

least one memory 103. *Id.*, 4:13-17, 4:35-37. Memory 103 stores message data 107 (“a set of promotional messages associated with a set of entities or clients”), user data 108 (“user phone number, user device identifier, other information identifying the user or the user mobile device,” and the user’s status as a new or existing user), and client data 109 (user white lists and black lists “associated with a set of clients/entities” as well as client preferences and business rules). *Id.*, 4:43-54.

124. Client server 130 is associated with a client (also identified as an “entity” or “vendor”), which Long describes as “selling or providing a good(s) or service(s) via the internet, and/or engaging in any marketing activities via the internet.” *Id.*, 5:38-42, 6:34-37.

125. User mobile device 150 is any mobile electronic device, including “a mobile phone, a tablet, a smart watch, a personal computer, a personal digital assistant (PDA), a smart phone, and/or the like.” *Id.*, 5:48-52.

126. Long also describes an integration tag. Memory 103 of the click-to-text server “can store code representing integrator instructions 105 (i.e., integration tag) to be executed by the at least one processor 101 or the user mobile device 150.” *Id.*, 4:63-66. The click-to-text server “can send an integration tag ... to the client server,” and the tag “includes code, when executed, cause the user mobile device to send a request to the click-to-text server and receive from the click-to-text server

promotional messages associated with the client.” *Id.*, 11:23-29. The tag “can be attached to a page load event at the user mobile device,” so that “[w]hen the user is opening a page (e.g., a webpage) associated with the client, the request for the promotional message can be sent to the click-to-text server.” *Id.*, 11:23-31.

127. When the integration tag executes, the user mobile device “can generate a unique visitor identifier and store 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.*, 11:46-50. Execution of the tag also “sends to the click-to-text server user data,” which Long lists as including “user phone number, user device identifier, other information identifying the user or the user mobile device, user viewing history, user click/tap history, user status (a new user or an existing user), user cookies, page referrer URLs, impression data, [and] a user agent field collected by the web browser.” *Id.*, 11:53-60.

128. The click-to-text server also receives selections made at the user mobile device and serves pages on its own domain. Long provides “[a]n example HTTP form that POSTs to the client-to-text server.” *Id.*, 9:6-7. And Long states that a user preference page “can use the same client_domain.attn.tv domain specified in the site integration tag.” *Id.*, 11:19-21.

129. Users interested in receiving marketing information from a client can select a “sign-up” link displayed on the client’s webpage and request a subscription.

Id., 3:10-15, 6:58-7:21. Selecting the link launches the user’s messaging application and pre-populates a text message to the client’s telephone number with the request, which the user sends to subscribe. *Id.*, 3:10-15, 6:58-7:21.

130. After the user requests a subscription, the click-to-text server receives a user identifier, such as “a user phone number, a sender phone number, [or] a device identifier of the user mobile device” the integration tag described above. *Id.*, 4:59-66, 7:42-56, 11:53-60. The click-to-text server then authenticates the user based on the user identifier. *Id.* As part of the authentication process, the click-to-text server checks the client’s blacklist or whitelist. *Id.*, 7:57-8:5. If the user is not on a blacklist, or is on a white list, the user is authenticated. *Id.* The server will then provide the user service or send the user promotional messages. *Id.*

131. Figures 5A through 5I of Long apply a similar mechanism to purchases. To start, a customer viewing a shopping cart on a vendor’s website taps “1-Step Checkout” link 502. *Id.*, 14:50-15:5, Figs. 5A-5B. The customer’s messaging application then opens with a pre-populated purchase request 513 that can identify the shopping cart, the products, and their prices. *Id.* The request is addressed to the vendor’s telephone number. *Id.*

132. When the click-to-text server receives the message from the customer containing the request, it—similar to the process for a customer subscription—authenticates the user based on the user identifier and checks any black lists or white

lists. *Id.*, 15:30-41. In doing so, the click-to-text server uses the user identifier to determine whether the customer is new to the client or not. *Id.*

133. The click-to-text-server sends a customer a message based on whether they are a new or existing customer. A new customer receives message 522 requesting shipping and payment information along with a “checkout link” that “opens a third user interface with a checkout page 531.” *Id.*, 15:41-52, Figs. 5C-5D. An existing customer instead receives message 562 listing the products in the cart and message 563 informing the user of the shipping information and the payment information on file associated with the user, which can include a checkout link that, when clicked, opens a third user interface with a checkout page where the user can change the shipping and payment information. *Id.*, 15:56-63, Figs. 5G-5I.

134. The click-to-text server collects both customer and marketing data across transactions, which it stores in user data 108 within memory 103. *Id.*, 4:46-51, 16:6-12, 17:25-31. Customer data includes “the user’s payment information (e.g. credit card information, bank account information, or other information), shipping address, and preferred shipping-related settings,” which the click-to-text server uses “to provide a user-friendly purchase experience in subsequent transactions.” *Id.*, 12:65-13:7. Marketing data includes “the type of website content the user has viewed, what items the user has previously purchased, and/or the like.” *Id.*, 13:7-14. Long further states that “the user’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) can be stored in a user database of the click-to-text server.” *Id.*, 16:5-12. The click-to-text server uses this data when identifying an existing customer and sending that customer the shipping and payment information it has on file. *Id.*, 15:56-66.

135. Long also addresses the importance of secure transactions by disclosing two different security measures. First, each pre-populated message carries a unique fingerprint that the click-to-text server generates and appends to the message body as a reference, which in my opinion permits the server to associate an incoming message with the particular selection that produced it. *Id.*, 10:54-57. Second, Long contemplates supplementing the stored record with outside information, stating that the server may “append additional data, directly collected or through a third party . . . to the user’s phone number as a key value.” *Id.*, 13:14-19. Long identifies the purposes of that measure as “fraud protection” and disabling “a recently changed number.” *Id.*

2. U.S. Patent Application Publication No. 2012/0310752 to Gaddis

136. U.S. Patent Application Publication No. 2012/0310752, titled “System, Method, and Computer Program Product for Data Entry Free Electronic Purchasing” to Gaddis (“Gaddis”), was filed on June 6, 2011, and published on

December 6, 2012. EX1006 (Gaddis), Cover. I understand that Gaddis is therefore prior art to the '924 patent.

137. Gaddis was not cited by the applicant or the Examiner during prosecution of the '924 patent. EX1001, References Cited.

138. Gaddis, like the '924 patent, addresses marketing messages sent to consumers' electronic accounts. Gaddis explains that advertisements are sent "via email, SMS-text, Instant Messaging, Tweets, Facebook posts, and other emerging formats" by "Offer Providers (OP), who are either merchants or third party service providers representing merchants," and that responding to them on a smartphone "is very difficult, particularly when alpha numeric data input from a mobile keyboard is required." EX1006 (Gaddis), ¶¶3-4. Gaddis thus identified a need in the art "to authenticate the User prior to sending the advertisement, and then re-verify the authenticity of the User after they have placed a purchase," *Id.*, ¶5, and also sought to disclose a way for a user to have a secure, efficient, and accurate method to buy from the advertisement "without entering any alpha numeric data." *Id.*, ¶¶6-8.

139. Gaddis explains that the Offer Provider "is required to have the User's following information on file prior to sending the advertisement: contact information (e.g. email addresses), shipping information if required, and billing information sufficient to complete a financial transaction." *Id.*, ¶8. Gaddis repeats

that “[i]n all of the methods of the present invention,” the user “must have a ‘pre-existing’ account with the merchant.” *Id.*, ¶51. Gaddis defines its “User” accordingly, as “any person who receives promotional offers due to authentication through previous registration, account creation and opt in for promotions from Offer Provider.” *Id.*, ¶37.

140. Gaddis discloses that the advertisement contains 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. The PEL is “encrypted before sending to User and decrypted by OP,” and “has special capabilities to both properly direct User to offer as well as track and report on User actions.” *Id.*, ¶34. Users “are assigned a unique User ID” that is “encrypted by methods well known in the art,” and the link passes parameters that include “the User identification (encrypted).” *Id.*, ¶¶52, 57. Gaddis defines the “Service Provider” as an Offer Provider “who has been contracted by the merchant to transmit advertisements to Users (in lieu of the merchant), receive User’s electronic purchase orders, confirm User’s orders, and notify merchants to process orders and ship items.” *Id.*, ¶32. Such a provider “only needs to possess the specific contact information that is required to send the message to the appropriate account,” such as “a cell phone number if sending an SMS/Text.” *Id.*, ¶54.

141. Gaddis describes text messaging as a channel for the PEL itself, not merely as a notification option. Gaddis defines the “Electronic Communications Account” as “any User owned account including landline telephone, mobile phone, email, SMS, IM Instant Messages and posts, including social network accounts,” *Id.*, ¶27, and defines “link” as “any item on a webpage or an electronic communication (e.g. email link, SMS link, or link posted on a User’s social media site ...) that when clicked (i.e., activated), opens a connection,” *Id.*, ¶28. The method operates on an advertisement “sent from the Offer Provider to the User’s Electronic Communications Account (e.g., email, text-SMS, instant messaging-IM, and Social networking webpages),” within which “[t]he User clicks on a Promotionally Enabled Link (PEL).” *Id.*, ¶39. The parameters the system passes identify “which User’s Electronic Communications Accounts advertisement is sent (e.g. email, SMS, Social networking account) (LinkChannels),” *id.*, ¶57, and, upon purchase, “which link channel the purchase was made from (e.g. email, SMS, IM, Facebook®, Twitter®) (LinkChannelAccepted),” *id.*, ¶64.

142. Gaddis also shows the encrypted link arriving in a text message. Where a User elects text confirmation, “they will receive a text message as demonstrated in FIG. 7 comprising the same PEL and option to cancel the order.” *Id.*, ¶62, Fig. 7. Gaddis states that “[m]ethods of emailing, texting, posting, and instant messaging to electronic communications devices are well known in the art,”

id., ¶50, and that although certain preferred embodiments are described with advertisements sent via email, “other embodiments that are apparent to those of ordinary skill in the art (e.g. advertisements sent via SMS, IM instant messaging, and electronic messages or posts sent to Social networking accounts) ... are also within the scope of this invention,” *id.*, ¶65.

143. Clicking the PEL opens a page built for the user. The information passed to the service provider “enables the service provider 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 the service provider “can also create a webpage specific to each User’s requirements ... by methods well known in the art.” *Id.*, ¶58. The page “addresses them by their name or a unique greeting, describes the product or service, and optionally, the quantity that may be purchased,” and the user completes the purchase in a few clicks “while not being required to (log in or) enter any of their personal data.” *Id.*, ¶¶48-49, Figs. 2A-2B.

144. Gaddis’s PEL is unique to each user. Each user is “assigned a unique User ID that may be provided to third party service providers,” and “[t]his unique User ID is encrypted by methods well known in the art.” EX1006 (Gaddis), ¶52. The link includes parameters identifying the deal, the merchant, and the user. For instance, Gaddis explains that “‘custhash=9098788492’ is the encrypted User identification (UserId) specific to the User,” and the programming code “include[s]

a module for the merchant or Offer Provider to encrypt and decrypt the UserIds as needed.” *Id.*, ¶¶57, 59-60; see also *Id.*, ¶53, claim 19 (“encrypted links unique to each User”), claim 5.

145. Figure 4B of Gaddis, reproduced below, depicts the sequence of one of its embodiments. The service provider sends an advertisement to established users; “[i]f the User clicks (click 1) on the PEL embedded within the communication 430, then they will be re-directed to a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User”; the user places and confirms the order; and the service provider notifies the merchant “so that they may process the User’s order and payment.” *Id.*, ¶59, Fig. 4B.

146. Gaddis treats control over who may use the PEL as a feature of the invention. Gaddis states that “[a]nother feature of the present invention is secure and improved purchase order accuracy by preventing a person, who is not the original User that received the Offer Provider’s electronic advertisement, from charging the User’s financial accounts.” *Id.*, ¶10. Gaddis defines a “Non-User entity” as “any individual or organization of individuals engaging in unauthorized billing of a User’s financial accounts, such as those involved in identity theft or friends of a User to whom the User has forwarded a promotional message.” *Id.*, ¶31.

147. Gaddis describes what happens when someone other than the intended user activates the PEL. Where the original user “voluntarily shares the advertisement with a Non-User entity, for example by forwarding an email to a friend, when the friend attempts to place an order, they will be directed to the Offer Provider’s other venues for electronic purchasing.” *Id.*, ¶10. Gaddis explains the mechanism: “[w]hen the receiver clicks on the hyperlink, the same webpage will open as for the original intended User,” but that page carries “a personally identifiable statement ... such as ‘Hello User First Name, if you are not {User First Name}, then click here to purchase the product,’” and clicking that link “will take them to a page where the receiver can start the authentication and payment process via the merchant’s normal Internet purchase procedure.” *Id.*, ¶59. Where a Non-User entity “accidentally or fraudulently attempts to bill the original User,” a confirmation is sent to the original user, “wherein the User would decline the purchase by not clicking on the embedded link.” *Id.*, ¶10.

148. Gaddis applies the same protection to text messages. Gaddis states that “when an Offer Provider sends an SMS/text to a User, who then forwards it to a Non-User entity such as a friend via SMS or email, the order confirmation will be sent from the Offer Provider to the User’s SMS/Text account, and not to the friend’s SMS or email account.” *Id.*, ¶50.

149. Finally, Gaddis describes an alternative in which the PEL takes the user to the merchant's own webpage. *Id.*, ¶60. Gaddis separately describes an "ECA Single Click Method" that "is applicable for a User whose identity has been previously verified by the Offer Provider." *Id.*, ¶61. Gaddis states 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.* Gaddis adds that "[m]ethods of credentialing are well known to those of skill in the art of electronic communications," and that "[i]n the digital environment, a credential is a data structure or an electronic document which has a defined structure known to all involved parties, and is issued by an authority." *Id.* Gaddis also describes a "double opt-in confirmation" in which the user chooses to confirm by email, SMS, or telephone call, *Id.*, ¶¶12, 62-63.

150. Gaddis thus describes sending a consumer, by email or text message, a link that is unique to that consumer and opens a page created for that consumer, from which the consumer completes a purchase. Gaddis further describes verifying that the consumer was authenticated before the message is sent, and directing anyone other than that consumer to ordinary checkout.

3. Motivation to Combine Long with Gaddis

151. In my opinion, a POSITA would have been motivated to combine Long and Gaddis. Specifically, a POSITA would have sought to combine Long's SMS messaging and checkout architecture and flow with Gaddis' secure Promotionally Enabled Link (PEL). That combination would take advantage of the integrated e-commerce messaging and customized webpage disclosures of Long, while incorporating the security techniques of Gaddis to maintain the confidentiality of customer information in e-commerce transactions. I explain the basis for my opinion below.

152. Long describes a three-entity e-commerce configuration, where a click-to-text server sends a text message to a customer seeking to complete a purchase on an e-commerce website. EX1005 (Long), 15:40-61. The message—which the server sends on behalf of the e-commerce merchant—includes a custom link to a webpage comprising the user's shopping cart and stored shipping and payment information so that the user can complete the transaction. *Id.* In my opinion, a POSITA would recognize that such a 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 for securing user payment and shipping information to complete

the transaction in general terms, and Gaddis describes a specific technique for doing so.

153. To prevent unwanted disclosure of the customer's information, Gaddis' messaging and checkout configuration builds a secure link to send the customer from three parameters, a merchant identifier, a deal identifier, and an encrypted User identifier. Gaddis further describes encrypting the link before sending it. EX1006 (Gaddis), ¶¶34, 57-59. The service provider creates the webpage that link opens using that same information. *Id.* Gaddis contemplates delivering 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. Thus Gaddis' teaching would indicate to a POSITA that adopting Gaddis's link in Long's system would not need to change the text messaging channel Long uses.

154. 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 (Long), 4:1-11 (defining "data" to include "usernames, passwords," "banking transaction information (e.g., credit card information, back [sic] account information, etc.)," 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" used "for fraud protection or to disable a recently changed number"). In other words, Long's disclosures make clear that security surrounding the sensitivity of the data the platform handles was a concern, and Long discloses ways to address that risk.

155. Gaddis describes its encryption as both well-known and flexible, i.e., applying standard encryption techniques "well known in the art" and available this combined configuration. Gaddis states that "[t]he present invention may be implemented in a variety of scenarios," including where "third party service providers may represent various Offer Providers in advertising and processing of purchasing," 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 (Gaddis), ¶52; *id.*, ¶60 (software "enables a merchant to incorporate programming code into their electronic communications that they are sending to select Users" and includes "a module . . . to encrypt and decrypt the UserIds as needed"). A POSITA would thus recognize that Gaddis teaches that its encrypted identifier operates in the arrangement described by Long.

156. 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—namely using links delivered by SMS

messaging to give a consumer access to customized webpages for completing online transactions—and each aims to address the problem the '924 patent identifies, that static webpages produce a cumbersome user experience, which decreases 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. Long sends the consumer a text message containing a link that opens a checkout page built around that consumer's own transaction, displaying an order summary of the items in the consumer's cart. EX1005 (Long), 15:41-65, FIGS. 5A-5D, 5G-5H.

157. Long discloses, in general terms, the need for a mechanism to protect user information, and Gaddis provides such a mechanism, protecting user information in e-commerce-related message using its PEL, which directs the consumer “to a webpage hosted by the service provider and created specifically for the merchant's advertisement and the User.” EX1006 (Gaddis), ¶¶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 when completing such purchases.

158. Encrypting the checkout link as Gaddis describes would be a straightforward change for a POSITA. Both references disclose ecommerce 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. EX1005 (Long), 4:66-5:3, 7:57-8:5, 13:5-19, 15:56-16:5, 16:40-17:31, FIG. 1; EX1006 (Gaddis), ¶17, FIG. 4A. A POSITA would thus have understood that the "click-to-text" server of Long that generates the checkout link could have incorporated the encryption processes disclosed in Gaddis, for example, by making the checkout link a PEL carrying an encrypted user identification. EX1006 (Gaddis), ¶¶58-59, Figs. 2A-2B, 4B, 10. In other words, the 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 (Long), 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. No additional component is required at the client server or at the customer's mobile device, no additional message is sent, and no additional information is stored.

159. Moreover, as described above and incorporated herein by reference, using encryption to secure a link that includes or directs the user to sensitive information was a well-known technique, disclosed in several analogous prior art references and recognized in the industry as a way to improve security in mobile e-commerce solutions. *Supra* Section IX.A.2.b. Gaddis itself describes sending email links or SMS links that are "encrypted before sending to User and decrypted

by” the offer provider. EX1006 (Gaddis), ¶¶ 28, 34. Wendkos describes “encrypted URL[s] which can only be viewed by the recipient.” EX1023 (Wendkos), ¶37. Killoran describes the same practice carried out over SMS, generating “a short URL that corresponds to the short token and the long token,” then generating “an SMS offer or social media post offer message with the short URL Link” and sending it to the customer’s device, where the underlying tokens “may be encrypted or plain text strings which contain information to perform a transaction” and “information used to perform or authenticate a transaction.” EX1010 (Killoran), 7:48-52, 18:58-62, 31:49-55. Killoran adopted that approach to address known security problems with SMS, which it describes as “easily hacked.” *Id.*, 1:62-63. Industry standards reflected the same understanding: the Payment Card Industry Security Standards Council’s “Best Practices for Securing E-commerce” treated “encrypted transmission” of “cardholder data . . . across open, public networks” as paramount. EX1024 (PCI SSC), 31. 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, to protect user information, and would readily have had the knowledge to implement it.

4. Independent Claim 1

a. Long Discloses 1 ``` [pre] ```

160. To the extent the preamble is limiting, Long discloses “[a] **computer-implemented method.**” Long describes “a click-to-text process 700,” shown in Figure 7, which “can be executed at, for example, a processor at a server such as the processor 101 of the click-to-text server 100.” EX1005 (Long), 2:13-14, 17:32-41, Fig. 7.

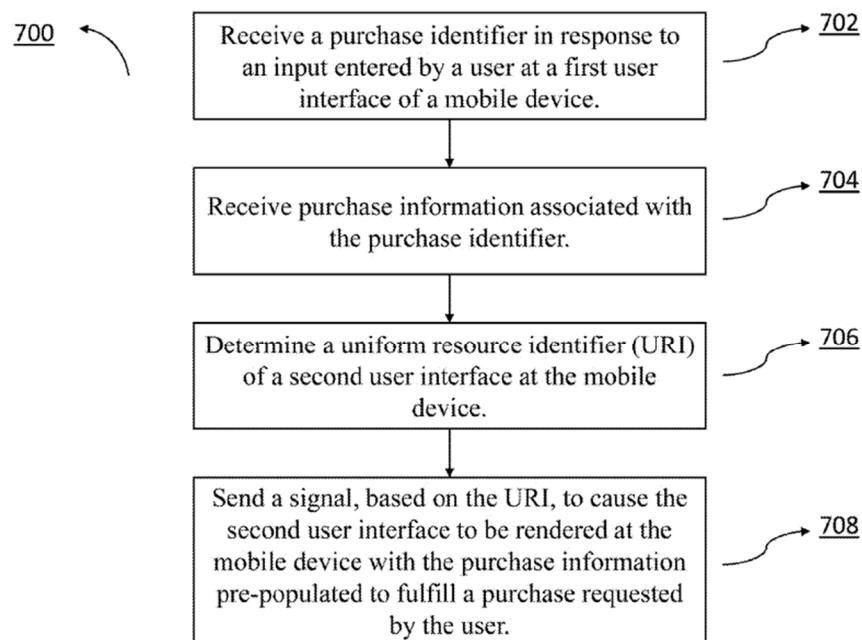


FIG. 7

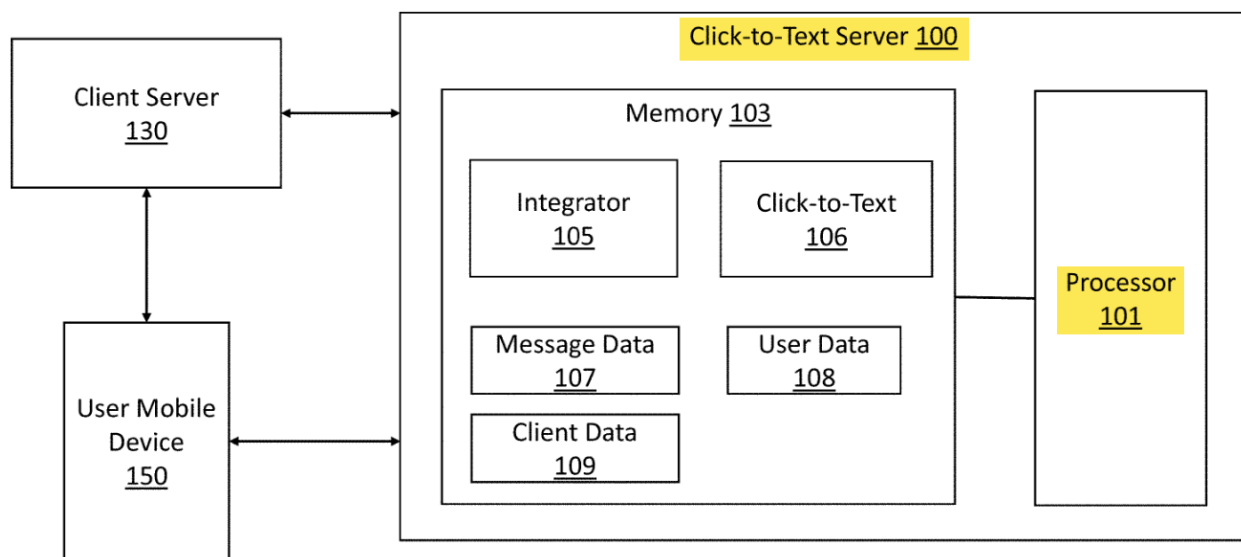


FIG. 1

161. The click-to-text server “can be or include a computer” and includes “at least one processor 101 and at least one memory 103,” where memory 103 stores “click-to-text instructions 106 to be executed by the at least one processor 101.” *Id.*, 1:62-64, 4:13-17, 4:32-38, 5:3-7, Fig. 1 (annotated). A POSITA would have understood that Long’s process, executed by a server processor running stored instructions, is a computer-implemented method.

b. Long Discloses 1[a]

162. 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.**” In my opinion, the “service subscriber” is the customer who subscribes to a vendor’s messages, the “telephone

number” is the customer’s telephone number, the “additional content” is the vendor’s marketing and purchase messages, and the “authentication information” is the user identifier that the customer’s device sends the server.

163. To subscribe to receive marketing information from a vendor, a customer taps sign-up link 203 on the vendor’s web page and sends the resulting pre-populated message 213 to the vendor’s telephone number. EX1005 (Long), 6:58-7:35, Figs. 2A-2B. The server stores “the user’s subscription status associated with the client” in user data 108, along with the “user phone number,” confirms the subscription by text message 222, and can then “provide service and/or send promotional messages 223 to the user.” *Id.*, 3:10-13, 4:46-48, 7:35-41, 7:62-67, 8:6-21, Fig. 2C. Because the subscription is created by a text message sent from the customer’s phone and the subsequent messages are text messages sent to the customer’s phone, the subscriber is associated with and receives the additional content at that telephone number. A POSITA would have understood that by recording the customer’s subscription status with the customer’s phone number and then sending the vendor’s messages to that number, the server configures the service subscriber to be subscribed to receive additional content at the telephone number.

164. Long also discloses that the server subscribes the user “in response to determining that the service subscriber has previously provided authentication

information.” When the customer taps the sign-up link, the customer’s device sends the server an HTTP POST request that 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.*, 8:55-9:1. Then, “in response to receiving the message 213, the click-to-text server can authenticate the user based on a user identifier,” and “the click-to-text server can receive the user identifier prior to receiving the message 213,” including in response to execution of the integration tag on the vendor’s page. *Id.*, 7:42-56. Authentication occurs if the user is not on a black list or is on a white list, after which the click-to-text server will send the customer marketing information. *Id.*, 7:57-67. A POSITA would have understood that the server’s authentication of the customer from a user identifier the consumer previously supplied before subscribing the customer and sending marketing messages is a determination that the service subscriber has previously provided authentication information, and that the subscription is configured in response to that determination.

165. Long’s checkout process also discloses this limitation. When the consumer sends purchase request 513, the server “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 message 563 “informing the user of the shipping information and the payment information on file associated with the user,” with a checkout link. *Id.*, 15:56-66, Fig. 5G. A POSITA would have understood that the server’s determination that the consumer is an existing customer from the user identifier is a determination that the customer has previously provided authentication information, and that the server then configures that consumer to receive the checkout messages at the consumer’s phone number in response.

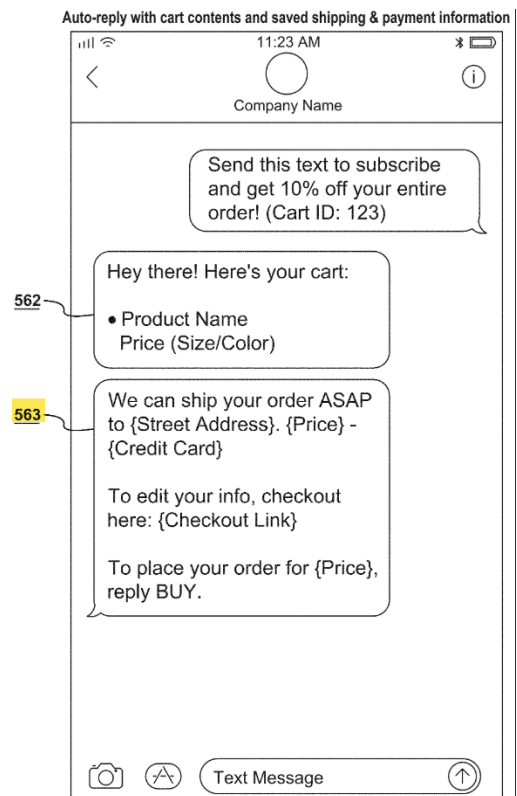


FIG. 5G

166. Long’s white list confirms this. A customer can be on a vendor’s “white list” only if the customer has previously provided information that put the consumer on the list, and Long sends messages only after customer opt-in to ensure “compliance with the Telephone Consumer Protection Act (‘TCPA’) and

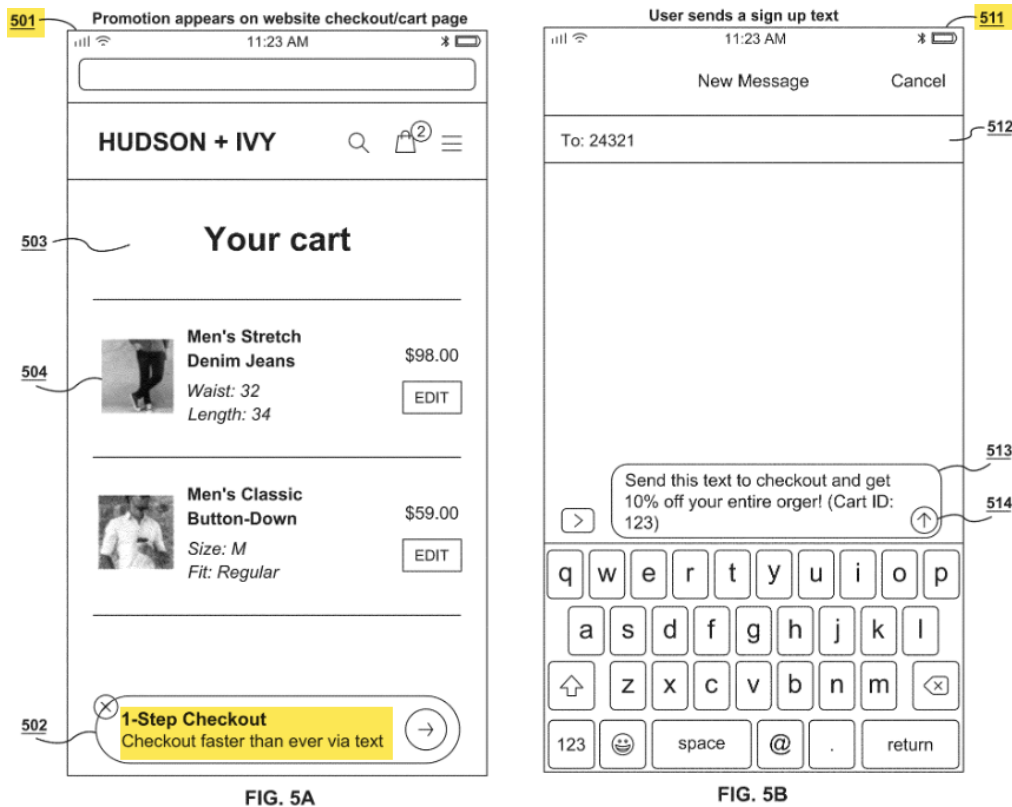
the regulations by trade associations representing the wireless communication industry (e.g., CTIA).” *Id.*, 6:53-57, 15:36-38. In my experience, a marketing “white list” was commonly understood at the time as a list of recipients who had consented to receive a sender’s messages. *See, e.g.*, EX1031 (defining “white list” as “a database containing email addresses whose owners have consented to receive marketing messages”); EX1032 (“Address book whitelisting happens when a subscriber adds your organization’s ‘from’ email address to his or her email contacts/address book, which in turn alerts their email service provider that they really want to receive messages from your address.”).

c. Long in View of Gaddis Discloses 1[b]

167. The combination of Long and Gaddis renders obvious the limitation **“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.”**

168. 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).



169. The click-to-text server sends the user messages via the second user interface (i.e., 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 a new customer, 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. EX1005, 15:41-55, FIG. 5C (annotated below). 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. EX1005, 15:56-16:2, FIG. 5G (annotated below).

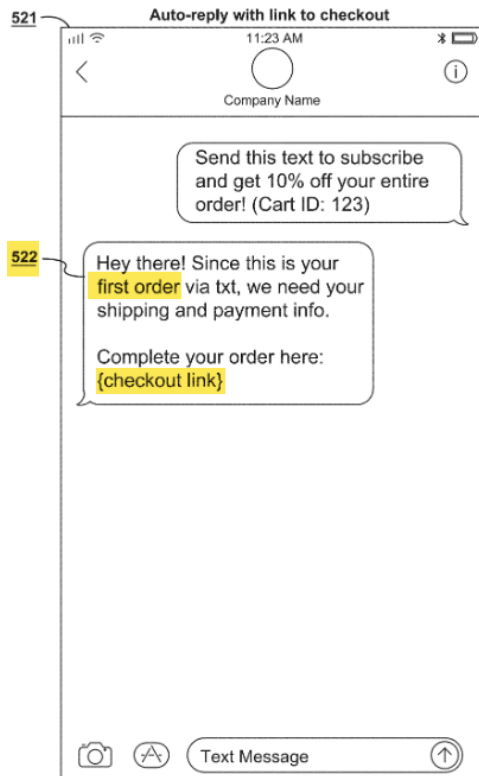


FIG. 5C

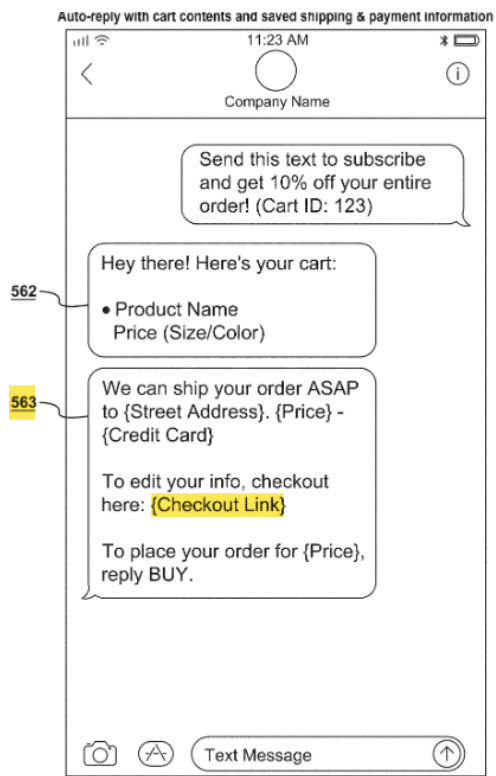


FIG. 5G

170. Messages 522 and 563 include a “checkout link” that, when clicked, opens a third user interface for the user—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 their 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 displays order confirmation page), 15:53-55 (click-to-text server sends a message

531

FIG. 5D

confirming the order has been placed); *see also* EX1005, 12:65-13:7 (describing storing user payment information), 17:3-8, FIGS. 5C, 5D, 5G.

171. 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. 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. 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, claim 5.

172. A POSITA would have further 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. EX1005, 15:45-47, FIGS. 5C-5D.

173. Long alone or in combination with Gaddis renders obvious “**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.

174. A POSITA would have found the “activating [of the one or more customized webpages] comprising generation of secure access information for performing the e-commerce transaction,” to be obvious in light of Long alone. Long explains that disclosing user information should be avoided, and 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 screening 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.

175. Even if Long did not disclose “the activating [of the one or more customized webpages] comprising generation of secure access information for performing the e-commerce transaction,” Gaddis does. *Id.*

176. 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. 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,” and can include promotional information including the User ID number, promotional offer, and target URL. *Id.*, ¶¶34-35, 59.

177. A POSITA would understand 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. Gaddis’ “webpage document generation module 410” creates the webpage included in the PEL. *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.” *Id.*, ¶59. The encrypted custhash identifies which User that page is for. *Id.*

178. A POSITA would recognize Long could be modified such that its SMS checkout link (the customized actionable item) incorporates the security characteristics of Gaddis’ PEL. In such a combination, Long’s click-to-text server is modified to generate the checkout link it sends in message 563 as a Promotionally Enabled Link built from a merchant identifier, a deal identifier, and an encrypted user identifier, to encrypt that link before transmission, and to

generate the checkout page that link opens using that same information. EX1005, 15:56-66, FIG. 5G; EX1006, ¶¶34, 57-59.

179. In the combination, when the subscriber taps the PEL in the text message displayed in Long's messaging application the link "redirects to the service provider," which here is Long's click-to-text server. EX1006, ¶59; EX1005 (Long), 11:18-21, 15:56-65. The click-to-text server decrypts the link, which Gaddis states is "decrypted by OP to facilitate purchase," yielding "?deal=123," "?merchant=xyz," and "custhash," the "encrypted User identification (UserId) specific to 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 (Long), 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." EX1006, ¶¶53, 58, 59. The webpage is customized and specific to the subscriber based on the contents of the link. Gaddis explains that the information exchanged between the merchant and service provider (messaging server) "enables the service provider 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 that the service provider "can also create a webpage specific to each User's requirements." *Id.*, ¶58.

180. As stated above, a POSITA would have been motivated to make this combination in order to achieve the security objectives already stated in Long. *See, e.g.*, EX1005, 10:54-57, 12:65-13:19 (describing fraud protection and other security measures). A POSITA would recognize that incorporating Gaddis' encrypted PEL—which carries a user-specific encrypted identifier that the server decrypts to build the subscriber's webpage—would further this objective of making the user's checkout information secure and provided only to the end user. EX1006, ¶¶34, 58-59.

181. A POSITA would understand that 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 IX.A.2. 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.

182. A POSITA would have a reasonable expectation of success in making this modification. 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," *id.*, ¶39, and tracks "which link channel the purchase was made from (e.g., email, SMS, IM, Facebook®, Twitter®)." *Id.*, ¶¶8, 39, 59. Gaddis further makes clear that a User selecting text confirmation "will receive a text message as demonstrated in FIG. 7 comprising *the same PEL*." *Id.*, ¶62 (emphasis added). Gaddis teaches that this substitution is available, stating 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.

183. Furthermore, 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." Under the Long-Gaddis combination, the customized action item includes Gaddis' PEL characteristics. A POSITA would recognize that Gaddis teaches that its encryption technique is compatible with this requirement and thus could be applied to Long's messages. Gaddis' Offer Provider is required to have the User's contact, shipping, and billing information on file before sending the advertisement: contact information (e.g., email addresses), shipping information if required, and billing information "sufficient to complete a financial transaction." EX1006, ¶8. Thus, a POSITA would understand

that Gaddis 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 IX.C.4.d (limitation 1[c]).

d. Long Discloses 1[c]

184. 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.**”

185. As discussed in limitation 1[b], Long discloses a “customized actionable item” in the form of a “checkout link” that launches a checkout page (customized webpage) for the customer (service subscriber) when selected. Long further discloses that the checkout link corresponds to the claimed “prior actions.” It expressly discloses that 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, 12:67-13:7, FIG. 5G.

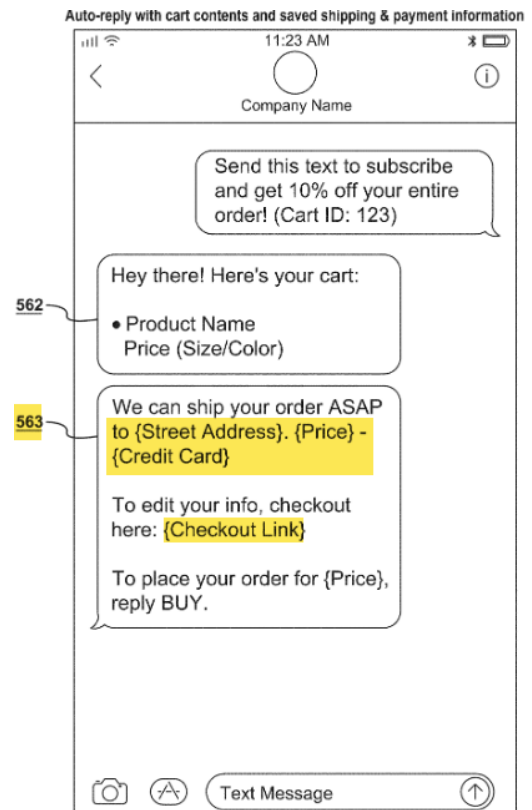


FIG. 5G

Further, during a subsequent click-to-text purchase process, the click-to-text server informs a user who is an existing customer of the shipping and payment information on file for them, and sends the user a checkout link showing a checkout page where the user can change that information. *Id.*, 15:56-16:12, FIGS. 5G-5H.

186. A POSITA would have recognized that by describing tailored messages based on prior transactions and including a link that opens to a checkout page that can be populated with information from a user's prior purchases, Long discloses a customized actionable item that corresponds to prior actions associated with one or more prior transactions performed by the user.

e. Long Discloses 1[d]

187. 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.”**

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

189. A POSITA would further understand that message 563 is a “third party message” because it is sent on behalf of the client—an entity, such as an e-commerce vendor—that is 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, and/or engaging in any marketing activities via the internet”), FIG. 1 (separating client server 130, user mobile device 150, and click-to-text server 100) (annotated).

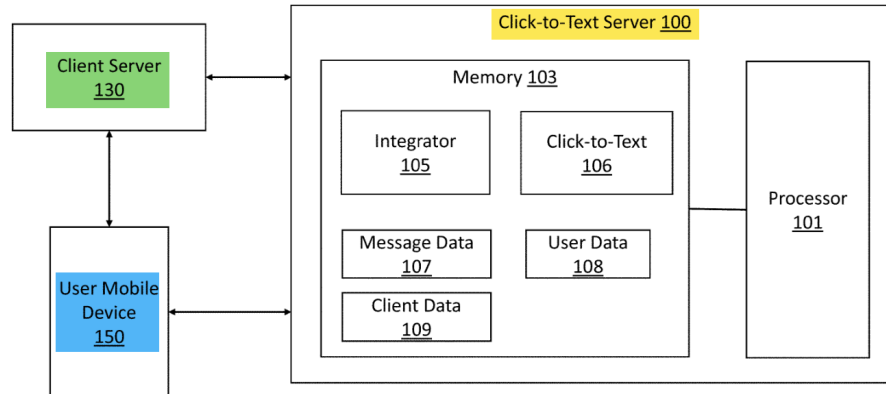


FIG. 1

190. Further, when clicked, the checkout link included in message 563 opens a third user interface that shows a checkout page for completing the user’s purchase with the client. *Id.*, 15:61-66. A POSITA would understand that the message is associated with the one or more customized webpages because it includes information about the checkout process the user is seeking to accomplish (e.g., shipping and product information), as well as a link to the custom checkout webpage.

191. The Long-Gaddis combination will be able to incorporate the encrypted checkout link. As discussed above, Gaddis resolves the encrypted link to redirect the user to a customized webpage. *Supra* Section IX.C.4.c (citing EX1006, ¶¶53, 58, 59). This further supports the compatibility of the prior art, and thus the reasonable expectation of a successful combination, and would further confirm for a POSITA that the checkout link (customized actionable item) is associated with the one or more customized webpages as claimed.

192. A POSITA would thus have understood that the click-to-text server that composes the message to send to the user generates for the user (“service subscriber”) a client (“third party”) message associated with the checkout page (“customized webpage”), where the client message includes the checkout link (“customized actionable item”).

f. Long Discloses 1[e]

193. Long discloses “**causing transmission of the generated third party message to the service subscriber.**” As described above, the click-to-text server sends (“causes transmission of”) message 563 (the “generated third party message”) to the user (“service subscriber”). Section IX.C.4.e (limitation 1[d]), *supra*.

5. Independent Claims 8 and 15

a. Independent Claim 8

(1) Long discloses 8[pre]

194. Long discloses “**a system.**” Long’s click-to-text system includes click-to-text server 100, client server 130, and user mobile device 150. EX1005, 4:32-38.

(2) Long discloses 8[a]

195. Long discloses “**a processor.**” Long’s click-to-text server 100 includes at least one processor 101. EX1005, 4:32-38, FIG. 1. Long further discloses that click-to-text process 700 is executed at processor 101. *Id.*, 17:32-41, FIG. 7.

(3) Long discloses 8[b]

196. Long discloses “**memory configured to store program instructions, wherein, when executed by the processor, the program instructions cause the processor to perform operations.**” 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.

(4) Long discloses 8[c]

197. For the reasons stated above for limitation 1[a], Long discloses limitation 8[c]. *See supra* Section IX.C.4.b.

(5) Long and Gaddis render 8[d] obvious

198. For the reasons stated above for limitation 1[b], Long and Gaddis render limitation 8[d] obvious. *See supra* Section IX.C.4.c.

(6) Long discloses 8[e]

199. For the reasons stated above for limitation 1[c], Long discloses limitation 8[e]. *See supra* Section IX.C.4.d.

(7) Long discloses 8[f]

200. For the reasons stated above for limitation 1[d], Long discloses limitation 8[f]. *See supra* Section IX.C.4.e.

(8) Long discloses 8[g]

201. For the reasons stated above for limitation 1[e], Long discloses limitation 8[g]. *See supra* Section IX.C.4.f.

b. Independent Claim 15

(1) Long discloses 15[pre]

202. 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 further explains that its implementations relate to a “non-transitory computer-readable medium” having instructions or computer code for performing computer-implemented operations, and that the

medium is 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.

(2) Long discloses 15[a]

203. For the reasons stated above for limitation 1[a], Long discloses limitation 15[a]. *See supra* Section IX.C.4.b.

(3) Long and Gaddis render 15[b] obvious

204. Limitation 15[b] combines the subject matter of limitation 1[b] with the subject matter that claim 2 adds to claim 1. Like 1[b], limitation 15[b] 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.”** Limitation 15[b] additionally recites 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”**—the limitation claim 2 adds to claim 1. EX1001, 20:66-21:3, 22:40-50. Long and Gaddis render each of those elements obvious for the reasons stated above for limitation 1[b] and below for

claims 2 and 9, which I incorporate here by reference. *See supra* Section IX.C.4.c (limitation 1[b]); *infra* Section IX.C.6.a (claims 2, 9).

(4) Long discloses 15[c]

205. For the reasons stated above for limitation 1[c], Long discloses limitation 15[c]. *See supra* Section IX.C.4.d.

(5) Long discloses 15[d]

206. For the reasons stated above for limitation 1[d], Long discloses limitation 15[d]. *See supra* Section IX.C.4.e.

(6) Long discloses 15[e]

207. For the reasons stated above for limitation 1[e], Long discloses limitation 15[e]. *See supra* Section IX.C.4.f.

6. Dependent Claims

a. Long Discloses Claims 2 and 9

208. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1 and 8, from which claims 2 and 9 depend. *See supra* Sections IX.C.4 (claim 1)-IX.C.5 (claims 8, 15).

209. 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.”

210. As noted above, in the Long-Gaddis combination, the “customized actionable item” is the Promotionally Enabled Link that the click-to-text server generated for the subscriber’s transaction from a merchant identifier, a deal identifier, and an encrypted user identifier, sent to the subscriber in message 563 as the “checkout link.” EX1005, 15:62-66; EX1006, ¶¶34, 58-59; *see also* Section IX.C.4.c. That link is associated with customized webpages, specifically 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.

211. 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 allows subscribers to directly access their checkout pages to complete purchases. EX1005, 15:45-52, 15:62-66; EX1006, ¶¶58-59.

212. 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.

213. Further, Gaddis expressly discloses that the PEL opens a webpage created specifically for the User and built from the User’s information on file, so that the User proceeds through a “no data entry” checkout process. EX1006, ¶¶48-49, 53, 58-60.

b. Long Discloses Claims 3, 10, and 16

214. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 3, 10, and 16 depend. *See supra* Sections IX.C.4 (claim 1), IX.C.5 (claims 8, 15).

215. 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 that the click-to-text server sends to the user via the client phone number are associated with the client, which is an entity or vendor selling or providing goods (e.g., tickets) or services (e.g., events) over the Internet. EX1005, 4:45-46, 5:39-42, 6:32-36. For example, promotional messages sent to users via the client (selling entity) can be “any advertising information related to a product or service that a client provides.” *Id.*, 6:66-7:4, 17:56-58. A POSITA would have thus understood that each such message is a “third party message”

“associated with a third party ticket provider, a third party service provider, or a third party event provider.”

c. Long Discloses Claims 4, 11, and 17

216. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 4, 11, and 17 depend. *See supra* Sections IX.C.4 (claim 1), IX.C.5 (claims 8, 15).

217. 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. Long discloses that 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.*, 4:45-54.

218. The content the subscriber receives includes messages containing 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 click-to-text 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.

d. Long in View of Gaddis Discloses Claims 5, 12, and 18

219. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 5, 12, and 18 depend. *See supra* Sections IX.C.4 (claim 1), IX.C.5 (claims 8, 15).

220. 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 in Sections IX.C.3 and IX.C.4.c, the “customized actionable item” is the encrypted Promotionally Enabled Link that the click-to-text server generated for the subscriber’s transaction, sent to the subscriber in message 563 as the “checkout link.” EX1005, 15:62-66; EX1006, ¶¶34, 58-59. As noted above, Long discloses sending a link to the subscriber to complete an e-commerce transaction, where the subscriber fills a shopping cart on a website, and then taps the checkout link so that the click-to-text server sends message 563 to the user 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.

221. 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.

222. A POSITA would have been motivated to secure Long’s checkout link with Gaddis’ encrypted PEL in order to protect the subscriber’s stored payment and shipping information that the link exposes, for the reasons stated in Sections IX.C.3 and IX.C.4.c, which are incorporated herein by reference. EX1005, 12:67-13:5.

223. For the reasons stated in Sections IX.C.3 (motivation to combine), IX.C.4.c (limitation 1[b]), which are incorporated herein by reference, POSITA would have had a reasonable expectation of success in making this combination.

e. Long in View of Gaddis Discloses Claims 6, 13, and 19

224. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 6, 13, and 19 depend. *See supra* Sections IX.C.4 (claim 1), IX.C.5 (claims 8, 15).

225. Long in combination with Gaddis renders “**wherein the authentication information comprises an authentication cookie configured to**

be stored on an electronic device associated with the service subscriber”

obvious.

226. As noted in limitation 1[a], the “authentication information” in Long is the “user identifier” that the subscriber’s mobile device supplies to the click-to-text server when the subscriber selects the “sign-up” link. *Supra* Section IX.C.4.b; EX1005, 8:55-59, 8:65-9:1. In addition, Long discloses placing a cookie on the user device that works with Long’s integration tag. Long’s integration 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.” EX1005, 11:23-31, 11:46-50. When the tag executes, it “sends to the click-to-text server user data” that includes “user cookies” in the same list as “user phone number, user device identifier, [and] other information identifying the user or the user mobile device.” *Id.*, 11:53-60. Long thus discloses a cookie on the user’s device that, upon the integration tag firing at a merchant website, is sent to the click-to-text server along with user identification information.

227. 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.

228. In Gaddis, the “User” is someone “whose identity has been previously verified by the Offer Provider.” EX1006, ¶61. The verification occurs after 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 that Gaddis discloses a cookie that resides on the User’s device as a record that the User was authenticated. *Id.*, ¶¶37, 61.

229. A POSITA would have been motivated to verify the subscriber from the cookie on Long’s device that is returned to the server, so that the cookie serves as authentication information with the user identifier, as disclosed in Gaddis. EX1005, 7:43-48, 11:46-50, 11:53-60. A POSITA would have had a reasonable expectation of success, because the modification uses a cookie Long already discloses and uses before opting-in to further messages (i.e., 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, [0061]. Thus, the result would be a combination of prior art elements according to known methods to yield predictable results.

f. Long Discloses Claims 7, 14, and 20

230. As discussed above, Long in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 7, 14, and 20 depend. *See supra* Sections IX.C.4 (claim 1), IX.C.5 (claims 8, 15).

231. Long discloses that **“the third party message comprises a Short Message Service (SMS) message or a Multimedia Message Service (MMS) message.”** Long discloses that the 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 or Verizon. EX1005, 7:11-21, 9:45-10:65, 11:1-10. A POSITA would have understood this functionality supports “third party messages” that “comprise[] a Short Message Service (SMS) message.”

232. Long also discloses that second user interface 601 displays a client’s promotional image 602 and promotional message 603 to the user. EX1005, 16:40-46, FIGS. 6A-6C. A POSITA would have concluded this functionality supports “third party” “Multimedia Message Service (MMS) message[s].”

D. Ground 2: Claims 1-20 Are Rendered Obvious by Louie in View of Gaddis and the General Knowledge of a POSITA

233. In my opinion, claims 1-20 of the ’924 patent are rendered obvious by Louie in view of Gaddis and the general knowledge of a POSITA. Louie in view of Gaddis and the general knowledge of a POSITA discloses or renders obvious

each element of independent claims 1, 8, and 15 and of dependent claims 2-7, 9-14, and 16-20.

1. U.S. Patent No. 10,360,627, titled “Systems and Methods to Provide Account Features via Web Based User Interfaces” to Anne Marie Louie et al.

234. U.S. Patent No. 10,360,627, titled “Systems and Methods to Provide Account Features via Web Based User Interfaces” to Anne Marie Louie et al. (“Louie”), issued from Application No. 14/106,380, filed December 13, 2013, and issued on July 23, 2019. EX1007, Cover. Louie claims the benefit of Provisional Application No. 61/736,986, filed December 13, 2012. *Id.* Louie published as U.S. Patent Application Publication No. 2014/0172660 A1 on June 19, 2014. *Id.* Because Louie’s non-provisional filing date of December 13, 2013 and June 19, 2014 publication date come before the priority date of the ’924 patent, I understand that Louie is prior art. Louie is assigned to Visa International Service Association and names Anne Marie Louie as its first named inventor. EX1007, Cover. Louie was not cited by the applicant or the Examiner during prosecution of the ’924 patent. EX1001, References Cited.

235. Louie describes a portal that sells credit card benefits to cardholders. Louie calls those benefits “account features,” and defines “[e]nhancement features” as “typically services or goods that a card issuer provides in addition to processing purchase transactions.” *Id.*, 1:52-55. The examples Louie gives include “zero

liability from loss of card,” “extra warranty period and companion airline ticket.”

Id., 1:55-61. Elsewhere Louie refers to such a feature as a “product,” stating that a score of nine means “there is a very high likelihood that the account holder would purchase such product.” *Id.*, 11:48-49.

236. Louie states that “the portal (143) of the transaction handler (103) provides the centralized location to access the data related to and/or the benefits of the features.” *Id.*, 6:19-21. Louie describes the transaction handler as the entity that “process[es] transactions between an acquirer processor (147) and an issuer processor (145)” and that “acts as a switch between acquirers and issuers for routing messages therebetween for purposes of authorization, clearing and/or settlement of financial transactions.” *Id.*, 5:59-6:11.

237. Cardholders reach the portal from the issuer’s website. Louie’s Figure 19 depicts “a website of an issuer that presents issuer content related to the consumer account (146) issued to the user,” which “verifies the identity of the user, before presenting the issuer content to the user,” and which “contains one or more links (401) configured to refer the user to the portal (143) in a secure way.” *Id.*, 24:17-23, Fig. 19. “When the link (401) is selected, the web browser of the user is redirected to the portal (143) that presents a user interface customized based on the identity of the issuer and/or the user.” *Id.*, 24:23-26. The portal then “authenticate[s] the user 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 to sign in the portal (143).” *Id.*, 24:59-66.

238. The page the portal presents is generated for the individual cardholder. Louie claims a method of “automatically generating and transmitting to the web browser of the user a customized webpage” that “is separate from the website of the issuer” and that “is customized by displaying an identification of the user and the white label resources” of that issuer. *Id.*, 40:32-38. The specification describes the same operation, stating that “[w]hen the user is referred to the portal (143) by the website of the issuer ... 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 to customize the user interfaces for the user associated with the issuer.” *Id.*, 23:45-50. Those “white label resources” include “logo, label, text area and links.” *Id.*, 28:31-32. Louie explains that this “white label configurability ... allows the issuers to customize the labeling of the user interfaces such that the user interfaces can be perceived as part of the websites of the issuers.” *Id.*, 3:11-15.

239. Cardholders use the portal to subscribe to receive alerts about their benefits at a telephone number. On the screen 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,” and “the account holder is to select 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 to the account holder.” *Id.*, 13:2-12, Fig. 8. Louie states that “[t]he selected preferences of the account holder are stored in the data warehouse (149) for the notification engine (117).” *Id.*

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

FIG. 8

240. Louie selects what to offer a given cardholder from what that cardholder has already bought. The transaction handler “stores the transaction data (109) recording the transactions processed at the transaction handler (103),” and

that record “can be used to customize offers to the account holders.” *Id.*, 6:12-18.

The feature offer engine, which Louie describes as “coupled to the data warehouse (149) and/or the transaction handler (103),” “is to use the account information and/or purchase history to determine or identify a particular account holder based on some predetermined criteria.” *Id.*, 8:14-20, 8:46-49. Louie gives as an 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.*, 8:49-52. The engine then offers that feature “via a communication in the form of an email with a hyper-link to register for the offer, a mobile message, a text message, a voice message.” *Id.*, 8:58-61.

241. The resulting notifications reach the cardholder by text message. Louie states that “the notification engine (117) is to notify the account holder via an email, a text message, a voice message, etc. ... when the account holder is eligible for the offer of an account feature,” *id.*, 6:38-42, and that “[t]he notification of the optional purchase for the coverage ... is to be communicated to the targeted account holder via an email, a text/SMS message, a voice message,” *id.*, 9:8-12.

242. Louie then provides an exemplary disclosure about what the user can do with that notification. Louie states that “an example message sent to the account holder who had previously given permission to receive promotional offers

is ‘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.*, 16:19-21.

243. Alternatively, the cardholder may act on a link included in the text message. Louie states that “the account holder can also purchase the particular benefit offered by clicking on an ‘Activate’ link provided in the message,” and that “[t]he clicking 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.*, 16:22-26. From the portal 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.

244. Louie thus describes subscribing a cardholder at a telephone number, selecting an offer for that cardholder from that cardholder’s own purchase history, sending the offer to that telephone number by text message with a link, and opening from that link a portal page built for that cardholder on which the purchase is completed.

2. Motivation to Combine Louie with Gaddis

245. In my opinion, a POSITA would have been motivated to combine Louie and Gaddis. Specifically, a POSITA would have sought to combine Louie’s

architecture and flow 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. EX1007 (Louie), 13:2-12, 8:46-52, 8:58-61, 9:8-12, 16:22-26. This combination would take advantage of Louie's integrated offer messaging and customized webpage disclosures, while incorporating the encryption techniques of Gaddis to maintain the confidentiality of cardholder account information in e-commerce transactions. I explain the basis for my opinion below.

246. The design choices in Louie would have conveyed to a POSITA that a link of this kind should be secured. Louie protects each path of access to its portal that it describes. For example, before any account content appears, Louie confirms who the cardholder is. 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," *Id.*, 24:19-23. The portal authenticates that cardholder from "a parameter passed from the issuer site to portal (143) via the link (401)." EX1007 (Louie), 24:59-66. A cardholder who reaches the portal without that handoff must "present a user name and a password to sign in." *Id.*, 25:3-4. Louie also controls how data travels and who may ask for it, sending API traffic over "a Secure Socket Layer (SSL) channel" and verifying "that the request message is from a system

authorized to receive the requested data” before answering. *Id.*, 22:30-34. Louie also restricts what issuers may put into its pages, allowing customization only within “a predetermined set of parameters, but without the security vulnerability of unvalidated, uploaded HTML.” *Id.*, 24:5-6. A POSITA would thus readily expect that any link sent by SMS that returns the user to the customer portal would contain security measures.

247. Louie sends such a link by text message. Louie states that notifications are “communicated to the targeted account holder via an email, a text/SMS message, a voice message,” EX1007 (Louie), 9:8-12, that the offer “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.*, 16:19-21, and that the cardholder may instead purchase “by clicking on an ‘Activate’ link provided in the message,” which “brings the account holder to a page maintained by the web portal (143).” *Id.*, 16:22-26.

248. As explained above, Gaddis provides such security measures. To prevent unwanted disclosure of the customer’s information, Gaddis describes creating a link that includes an encrypted identifier “specific to the User” and encrypts that link “before sending to User.” EX1006 (Gaddis), ¶¶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. A POSITA adopting

Gaddis's link in Louie's system would understand that the modification would not require any change to the channel Louie already uses to reach the cardholder. Further, Gaddis explains that it is built to be implemented in systems like Louie's. It explains that a sender may add Gaddis' technique to a messaging operation it already runs, 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 is applied 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. In my opinion, that passage is directly on point here, because Louie's portal is operated by the transaction handler rather than by the issuer whose card is being used, and so is precisely the kind of third party Gaddis contemplates. EX1007 (Louie), 6:19-20.

249. Under the combination, Louie's portal would build the link it sends in an offer message as Gaddis's PEL, from a merchant identifier, a deal identifier, and an encrypted identifier of the cardholder, and would encrypt that link before sending it. EX1006 (Gaddis), ¶¶34, 57-59. When the cardholder taps the link, the portal would decrypt it and identify the cardholder, then present the customized page it already generates. EX1007 (Louie), 40:32-38.

250. In my opinion, 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 aims to address the purported 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 account holder disclosing, "automatically generating and transmitting to the web browser of the user a customized webpage" that "is customized by displaying an identification of the user," and presents them "in a user friendly way" so the cardholder reaches the offer without hunting for it. EX1007 (Louie), 40:32-38, 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 (Gaddis), ¶¶8, 58.

251. This combination of prior art elements employs known methods to yield predictable results. Louie protects access by authenticating users based on credentials included in issuer-website links, and the portal already handles encrypted traffic on its application programming interface channel. EX1007 (Louie), 24:19-23, 24:59-66, 22:30-34. The modification puts an encrypted

identifier into a different link pointing at that same portal. In my opinion, Louie’s portal is equipped to perform that operation because it already identifies a credential out of a link and authenticates the cardholder from it. *Id.*, 24:59-66. Gaddis further explains that the encrypted identifier is flexible and works “[i]n all scenarios” it describes, including where a third party sends the messages, using “methods well known in the art,” just as in Louie. EX1006 (Gaddis), ¶52.

252. Moreover, as described above, adding secure access information to a link that provides access to sensitive user information was a well-known technique in the e-commerce environment, particularly where the link directs to a credit card account and stored billing information. *Supra* Section IX.A.2.b (citing EX1006 (Gaddis), ¶34; EX1023 (Wendkos), ¶37; EX1010 (Killoran), 7:48-52, 18:58-62, 31:49-55, 1:62-63). Industry standards applied that understanding directly to payment card data. The Payment Card Industry Security Standards Council’s “Best Practices for Securing E-commerce” treated “encrypted transmission” of “cardholder data . . . across open, public networks” as important. EX1024 (PCI SSC), 31. Because the link in Louie’s offer message opens a portal page presenting the cardholder’s account features and the billing information from which the purchase is completed, a POSITA would have known that such a link required “secure access information,” such as an encrypted link, and would readily have had the knowledge to implement it. EX1007 (Louie), 16:22-26, 26:29-31.

3. Independent Claim 1

a. Louie Discloses 1[pre]

253. Louie discloses “[a] **computer-implemented method.**” Louie is directed 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, 1:26-30. It discloses a portal “configured to provide 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, [or] a call center for customer services” to “build applications tailored to their needs and preferences, using the centralized account feature data.” EX1007, 2:64-3:3. Louie also discloses a “computing apparatus” configured “to store account data (e.g., 133, 134) identifying account features (e.g., 127, 128) of a plurality of separate payment accounts,” to “receive data identifying a first payment account,” and to “determine whether a user of the first payment account . . . is eligible for a benefit of [an] account feature.” EX1007, 17:44-55.

254. A POSITA would have understood these disclosures—a data-processing apparatus, an API-accessible portal, and a computing apparatus that stores account data and determines feature eligibility—to disclose a computer-implemented method performing the steps recited in claim 1.

b. Louie Discloses 1[a]

255. Louie 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 discloses that “[t]he notification engine (117) can use a one-way or two-way communication to market the additional purchase ... to the account holder and/or to allow the account holder to either decline or cancel the purchase,” where the notification is “communicated to the targeted account holder via an email, a text/SMS message, a voice message, etc.” EX1007, 9:5-12. Louie’s Figure 8 “illustrates an interface showing options to set up notifications,” through which “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				
Text Message				
Voice Message				
				Continue

FIG. 8

256. “[I]n one embodiment, the account holder is to select 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 to the account holder.” EX1007, 13:6-12. “The selected preferences of the account holder are stored in the data warehouse (149) for the notification engine (117).” *Id.* Louie’s Figure 32 further discloses a “‘My Account’ page” that “include[s] a user interface configured to allow the user to provide and/or update user interface and/or preferences related to the consumer account, such as the address, phone numbers, email address, electronic disclosure preference, etc.” EX1007, 27:15-20, Fig. 32.

257. Louie discloses that “the portal (143) 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 itself “verifies the identity of the user, before presenting the issuer content to the user”—“the portal (143) is configured to authenticate the user based on a parameter passed from the issuer site to portal (143) via the link (401),” so that the portal “can automatically authenticate the user, based on the authentication performed by the issuer site and the parameter received from the issuer site via the link (401).” *Id.*, 24:17-23, 24:59-66. Either way, 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.
First Name
Last Name

Date of Birth
01
01
1901

Address:
Street Address
Street Address-2
City
State/Province
Zip/Postal Code
Country

Time Zone:
GTM (+8:00)

Home Phone:
Country
xxx-xxx-xxxx
Extention

Email:
Email Address
Re Enter Email Address

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:
Email Address
Not Confirmed
Resend Confirmation Link
Re Enter Email Address
The disclosures will be electronically delivered to this email address

Save
Cancel

FIG. 32

258. A POSITA would have understood that Louie's account holder is the service subscriber associated with a telephone number who the service subscribes to receive additional content because the account holder supplies a telephone number and elect to receive text message notifications of feature benefits, and that election is stored "in the data warehouse (149) for the notification engine (117)."

EX1007, 13:2-3, 27:15-19, FIGS. 8, 32. A POSITA would further understand that the configuring of that subscription occurs in response to determining the

subscriber previously provided authentication information because the interface to provide that information is inside Louie's portal, which the account holder must present a user name and password before reaching. EX1007, 24:19-20, 24:59-65, 25:3-4, 27:15-20.

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. Gaddis further explains that this "[p]rior verification"—i.e., sending a linked advertisement or checkout to a user after verification has happened—"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.*, ¶61.

260. A POSITA would be motivated to combine Louie and Gaddis for this purpose. Louie discloses that the issuer's 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, 24:21-40. The cardholder sets their notification preferences—i.e., opting in to receive text notifications—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. The “User” is defined by having opted-in to receive additional notification messages, which are 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” and the merchant or offer provider “must have previously acquired” the User’s billing and contact information before sending advertisement). In the combination, the cardholder subscribes to receive text messages through Louie’s portal, and the portal confirms the cardholder has opted-in and sends the offer only after confirming the cardholder was already verified.

261. A POSITA would have been motivated to make this combination in order to confirm that any text message with a link to the user’s account is sent only to a previously verified user, both for security and to ensure that billing information is on file so that purchases can be made seamlessly. This is a combination of 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. *Supra* Section IX.A.2. As noted above, because Louie’s portal is already responsible for authenticating user accounts and managing billing

information, it would be a reasonable modification to make sure that the phone number that receives the text belongs to the cardholder before sending the linked message. EX1007, 24:21-40.

c. Louie in View of Gaddis Discloses 1[b]

262. Louie 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.”**

263. Specifically, Louie’s portal generates a webpage for the individual cardholder (the “customized webpage”). Louie discloses “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. Further, “[w]hen the user is referred to the portal (143) by the website of the issuer of the consumer account (146) issued to the user, 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 to customize the user interfaces for the user associated with the issuer.” *Id.*, 23:43-50. Those “white label resources” include “logo, label, text area and links.”

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.

264. Louie discloses a “customized actionable item” included in the customized webpage. In one embodiment, Louie’s system sends a cardholder a message identifying a benefit that the account holder is eligible to purchase—for example, “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 message is transmitted to the account holder’s mobile phone, and the account holder 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 Louie’s “Activate” link included in the message to the cardholder is a “customized actionable item for performing an e-commerce transaction” because it is specific to the particular benefit for which the cardholder’s own prior purchase made the cardholder eligible, and because it links to and opens the portal page for performing the purchase of that benefit. EX1007, 16:22-26.

265. Louie further discloses that “[w]hen the user is referred to the portal (143) by the website of the issuer of the consumer account (146) issued to the user,

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 to customize the user interfaces for the user associated with the issuer”—i.e., the portal builds the webpage for the individual cardholder and uses “white label resources” to apply the issuer branding to the page. EX1007, 23:43-50. Louie claims the same operation, reciting “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.

266. Louie discloses activating the customized webpage “comprising generation of secure access information.” Figure 19 illustrates “a website of an issuer that presents issuer content related to the consumer account (146) issued to the user,” which “verifies the identity of the user, before presenting the issuer content to the user,” and which 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 “is configured to authenticate the user 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).” EX1007, 24:59-66. Louie applies the same discipline to its other channel by routing

application requests over “a Secure Socket Layer (SSL) channel over the network (101)” and “authenticat[ing] the requesting system, verifying that the request message is from a system authorized to receive the requested data.” EX1007, 22:30-36.

267. In my opinion, a POSITA would understand, or find it obvious based on the knowledge of a POSITA, that Louie’s “Activate” link in the SMS message to the account holder would have the same level of security. Louie secures every other path into the portal disclosed in the specification, and the page the “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. Encrypting such a link was a well-known technique that a POSITA would readily have had the knowledge to implement. *Supra* Section IX.A.2.b.

268. Even if Louie did not disclose this limitation, in my opinion, Gaddis does. As discussed in Ground 1 limitation 1[b], which is incorporated herein by reference, Gaddis discloses an “electronic message generation module 408” that 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; *supra* Section IX.C.4.c.

269. A POSITA would recognize Louie could be modified so its SMS “Activate” link (the customized actionable item) incorporates the security characteristics of Gaddis’ PEL. In such a combination, Louie’s portal (143) generates the “Activate” link it sends in the offer message as a Promotionally Enabled Link built from a merchant identifier, a deal identifier, and an encrypted user identifier, encrypts that link before transmission, and generates the benefit page that link opens using that same information. EX1007, 16:19-29; EX1006, ¶¶34, 57-59. When the cardholder selects the link, the portal decrypts it to resolve the encrypted user identifier against the account and billing information Louie’s portal maintains, and the cardholder is “re-directed to a webpage hosted by the service provider and created specifically for the merchant’s advertisement and the User,”—i.e., the purchase page for the cardholder benefit. EX1006, ¶59; EX1007, 16:24-29.

270. In my opinion, a POSITA would have been motivated to make this combination to achieve the security objectives Louie states. Louie authenticates every other path described in the specification into the portal and refers the user there only “in a secure way.” EX1007, 24:17-23, 24:59-66, 22:30-36. A POSITA would recognize that Gaddis’ encrypted PEL—which carries a user-specific encrypted identifier that the server decrypts to build the user’s webpage—further that objective for the one path Louie does not describe as secured. *See* EX1006,

¶¶34, 58-59. For the reasons given for the Long-Gaddis combination and above for Louie-Gaddis, this is a combination of 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, and a POSITA would have had a reasonable expectation of success—particularly because Gaddis expressly defines its PEL as an “email link, SMS link, or link posted on a User’s social media site” delivered to an account that may be “email, text-SMS, instant messaging-IM, and Social networking webpages.” EX1006, ¶¶39, 62; *see also supra* Sections IX.A.2.b (Secure Links), IX.C.3 (Long-Gaddis Motivation to Combine), IX.D.2 (Louie-Gaddis Motivation to Combine).

d. Louie Discloses 1[c]

271. 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 in limitation 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 discloses that the SMS message containing that link is triggered by prior actions associated with one or more prior transactions performed by the service subscriber (cardholder).

272. Louie discloses that its portal is designed to “trigger” additional transactions “in response to certain transactions qualifying for offers associated

with account features.” EX1007, 3:49-55. For example, Louie describes an account feature that provides premium trip-cancellation coverage. If the cardholder uses the account to buy an airline ticket that qualifies for that coverage but the account does not already have the feature, the system is triggered and notifies the cardholder “to enroll in the account feature,” i.e., purchase the insurance, with or without a fee. EX1007, 3:59-66; see also *Id.*, 8:34-52. A trigger may also be “an aggregated spending threshold” or “a predetermined number of transactions in a category, such as travel.” *Id.*, 9:59-10:10, 10:63-11:3, Figs. 11, 13.

273. The message that results from the trigger 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 (127), or when the account holder is eligible for the offer of an account feature.” *Id.*, 6:38-45. Louie confirms that “the applicable account feature is marketed via the notification engine (117) after a cardholder’s purchase of a qualifying transaction,” and that “[t]he qualifying transaction triggers One-on-One marketing to the cardholder for the appropriate ‘Feature.’” *Id.*, 7:63-8:5.

274. A POSITA would thus have understood that Louie’s “Activate” link corresponds to prior actions associated with one or more prior transactions

performed by the cardholder. The link is generated after a triggering event, such as the cardholder's prior purchase, aggregated spending, or number of prior transactions satisfying a feature rule; it is delivered in a message that identifies that qualifying purchase; and it opens a page for purchasing the related benefit for which the cardholder is eligible as a result. EX1007, 3:49-59, 9:59-10:10, 16:14-29.

e. Louie Discloses 1[d]

275. 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, 16:4-29. Louie discloses that this message is generated on behalf of, and describes an offer originating from, the issuer or feature provider associated with the account feature, i.e., a party distinct from both the service subscriber (the account holder) and the system performing the claimed steps (Louie's notification engine and portal). EX1007, 13:1-12, 16:4-29. A POSITA would have understood Louie's issuer or feature provider-associated notification, including an activation link tied to the customized webpage discussed for limitation 1[b], to be a third-party

message associated with the customized webpage and including the customized actionable item.

f. Louie Discloses 1[e]

276. Louie discloses **“causing transmission of the generated third party message to the service subscriber.”** As discussed above for limitation 1[d], Louie’s notification engine (117) generates the third party message and transmits it “via an email, a text/SMS message, a voice message, etc.” to the account holder’s phone number or email address on file. *See supra* Section IX.D.3.e; EX1007, 9:5-12, 16:4-29. A POSITA would have understood Louie’s SMS message to disclose this limitation.

4. Independent Claims 8 and 15

277. 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. Accordingly, for the reasons given above, Louie in view of Gaddis discloses 8[c] and 15[a] for the reasons given for 1[a]; 8[d] and 15[b] for the reasons given for 1[b]; 8[e] and 15[c] for the reasons given for 1[c]; 8[f] and 15[d] for the reasons given for 1[d]; and 8[g] and 15[e] for the reasons given for 1[e]. *See supra* Sections IX.D.3.b-IX.D.3.f.

278. As to 8[pre], and to the extent the preamble is held to be limiting, Louie discloses “[a] system comprising.” Louie discloses some “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, 1:26-30. It describes that “systems and methods are provided to trigger further transactions in response to certain transactions qualifying for offers associated with account features, such as a purchase to take advantage of the benefit of an account feature previously assigned to the account or the purchase of the account feature if it is not already in the account.” EX1007, 3:49-59. The various components of Louie’s system are depicted in Figure 1:

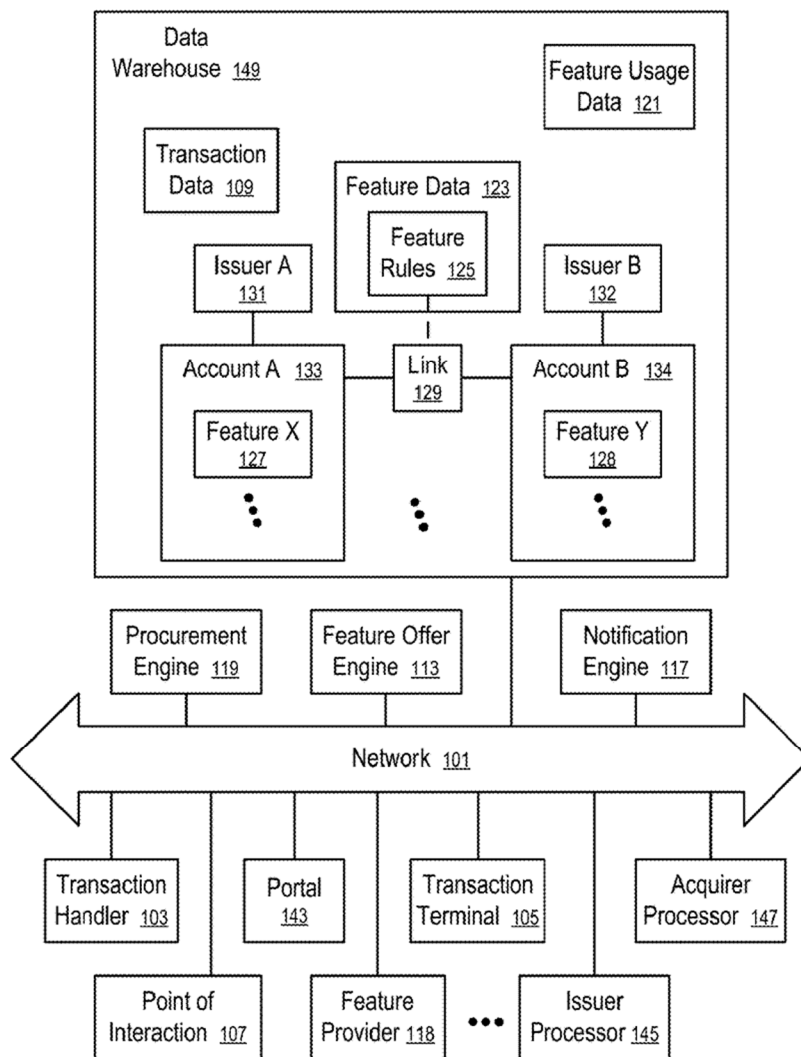


FIG. 1

279. 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. Louie explains that “the 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. In Figure 17, Louie explains “the data processing system (170) includes an inter-connect (171) (e.g., bus and system core logic), which interconnects a microprocessor(s) (173) and memory (167). The microprocessor (173) is coupled to cache memory (179).” EX1007, 37:43-64; see also *Id.*, cl. 10 (claiming “at least one processor, and a memory storing instructions configured to instruct the at least one processor to at least” perform the recited steps).

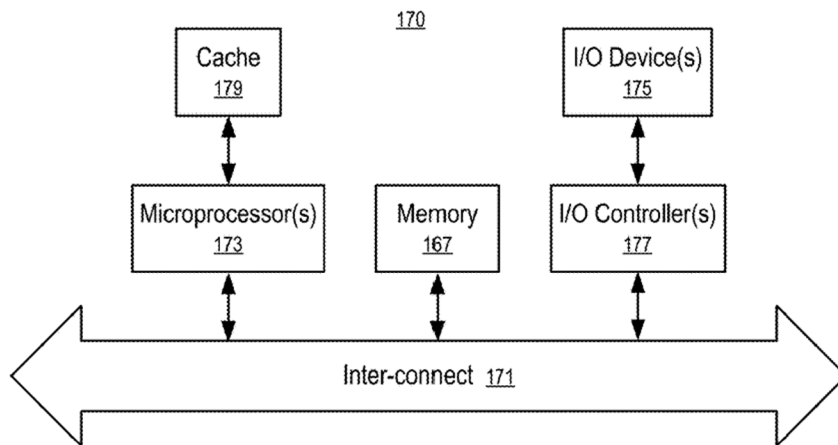


FIG. 17

280. As to 15[pre], and to the extent the preamble is held to be limiting, 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 above for 1[pre] and 8[pre] through 8[b]. *See supra* Sections IX.D.3.a,

IX.D.4. Louie further discloses that “a 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.” EX1007, 38:63-65. It explains that “[t]he executable software and data may be stored in various places including for example ROM, volatile RAM, non-volatile memory and/or cache.” EX1007, 38:65-39:1.

281. Limitation 15[b] differs from 1[b] in one respect. In addition to the operation recited in 1[b], limitation 15[b] recites 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, 22:40-50. That is the same subject matter claim 2 adds to claim 1, which recites 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.”** EX1001, 20:66-21:3. Because claim 15 recites that subject matter in its body rather than in a dependent claim, claim 15 has five dependent claims where claim 1 has six. My analysis of claims 2 and 9 below therefore supplies the showing for this additional element of 15[b], and I incorporate it here by reference: Louie’s “Activate” link data enables the account

holder to access the web-portal page to purchase an airline ticket feature or view its details, which a POSITA would have understood to be data configured to enable the service subscriber to purchase tickets, merchandise, or products or view the customized webpages depicting information about them. EX1007, 16:22-26; *infra* Section IX.D.5.a.

282. A POSITA would thus understand Louie in view of Gaddis renders claims 8 and 15 obvious.

5. Dependent Claims

a. Louie Discloses Claims 2 and 9

283. 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 in view of Gaddis render these limitations obvious.

284. As discussed above for claim 1, Louie discloses a “customized actionable item” in the form of an “Activate” hyperlink that allows a user to purchase additional account features. EX1007 16:21-26, 26:29-31, Fig. 24; *supra* Section IX.D.3.c.

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

b. Louie Discloses Claims 3, 10, and 16

286. 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.

287. As discussed above for limitation 1[d], Louie’s notification engine generates a third party message on behalf of the issuer or feature provider that links to the portal and purchase option pages. *See supra* Section IX.D.3.e. Louie discloses that “a portal is configured to provide 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, a call center for customer services, etc., to build applications tailored to their needs and preferences.” EX1007, 2:64-3:8, 5:42-59. Louie further discloses that “a network of approved feature providers (e.g., 118) or vendors are either a preferred suppliers of features or service providers and issuers,” and that “issuers . . . are to administer account features . . .

through a self service module.” EX1007, 14:38-46, 16:4-16:29. Louie also discloses the “trip-cancellation coverage” example tied to “an airline-ticket purchase” (EX1007, 3:49-67, 8:34-52), confirming that Louie’s feature providers include ticket-related service providers.

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

c. Louie Discloses Claims 4, 11, and 17

289. 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.

290. As discussed above for limitation 1[a], Louie discloses that the account holder selects notification preferences and a phone number via the interface of FIG. 8 to receive messages concerning feature benefits. *See supra* Section IX.D.3.b; EX1007, 13:1-12 & Fig. 8. Louie discloses that these messages originate from feature providers and issuers accessing the portal via APIs (EX1007, 2:64-3:8, 5:42-59) and that “the account holder is to select 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,” with “selected preferences . . . stored in the data warehouse (149) for the notification engine (117)” (EX1007, 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, 16:4-29.

291. A POSITA would have understood that when the cardholder sets his notification preferences, he is configuring his account to receive messages that will include offers from third party providers with the customized actionable item.

d. Louie in View of Gaddis Discloses Claims 5, 12, and 18

292. 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.

293. Louie’s disclosures identified for limitation 1[b] establish that Louie’s “Activate” link is a “secure link.” *See supra* Section IX.D.3.c. Louie secures every path into the portal, explaining that users reach the portal “in a secure way,” users are authenticated “based on a parameter passed from the issuer site to portal

(143) via the link (401),” and requests are routed 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, or found obvious, that the “Activate” link that opens the cardholder’s purchase page carries that same secure access information.

294. Even if Louie did not disclose this limitation, Gaddis does. For the reasons given for limitation 1[b], a POSITA would have found it obvious to modify Louie’s “Activate” link to incorporate the security characteristics of Gaddis’ Promotionally Enabled Link. *See supra* Sections IX.D.2, IX.D.3.c. In the combined configuration, the “customized actionable item” is the encrypted PEL that Louie’s portal generates for the cardholder’s offer and sends as the “Activate” link, and that link 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 to combine Louie and Gaddis in this manner, the known-technique rationale, and the reasonable expectation of success are set forth above and incorporated herein by reference. *See supra* Sections IX.D.2, IX.D.3.c.

e. Louie in View of Gaddis Discloses Claims 6, 13, and 19

295. 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.

296. As discussed above, Louie in combination with Gaddis discloses every limitation of claims 1, 8, and 15 from which claims 6, 13, and 19 depend. *See supra* Sections IX.D.2, IX.D.3, and IX.D.4.

297. As noted in limitation 1[a], the “authentication information” in Louie is the credential by which the portal (143) authenticates the account holder before the account holder reaches the notification and account-preference interfaces of Figures 8 and 32—either the “user name and a password” the portal may require the user to present “to sign in the portal (143),” or the “parameter passed from the issuer site to portal (143) via the link (401)” on which the portal relies to “automatically authenticate the user.” *Supra* Section IX.D.3.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 limitation obvious in view of Gaddis.

298. In Gaddis, the “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 that Gaddis discloses a cookie residing on the User’s device as a record that the User was authenticated. *Id.*, ¶¶37, 61.

299. A POSITA would have been motivated to use Gaddis’ cookie-based verification as the authentication information in Louie’s system, and would have had a reasonable expectation of success in doing so. Gaddis describes verification by cookies as a “method well known by the skilled artisan,” and Louie authenticates the account holder before presenting account information and authenticating 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 account holder’s device serves the same purpose Louie already describes, reducing friction in accessing the account feature, and requires no new components or message steps; Gaddis simply confirms this is done using a conventional browser mechanism—verifying by cookies. The motivation to combine Louie and Gaddis and the reasonable expectation of success set forth above are incorporated herein by reference. *See supra* Sections IX.D.2, IX.D.3.c.

f. Louie Discloses Claims 7, 14, and 20

300. 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.

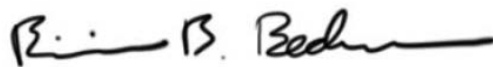
301. As discussed above for limitations 1[d] and 1[e], Louie discloses a “third party message” in the form of a “text/SMS message” that includes an “Activate” link to access an account feature. EX1007, 9:5-12, 16:4-29; see *supra* Sections IX.D.3.e-IX.D.3.f. A POSITA would have understood this to be a third party message comprising an SMS message.

X. CONCLUSION

302. For the reasons presented above, it is my opinion that the applied references render obvious claims 1-20 of the '924 patent.

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

Dated: October 19, 2026



Benjamin B. Bederson, Ph.D.