UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., AND
SAMSUNG ELECTRONICS AMERICA, INC.,

Petitioner,

v.

PAYGEO, LLC,

Patent Owner.

Case IPR2025-01555
Patent No. 12,014,347

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST

Exhibit	Description
Ex-1001	U.S. Patent No. 12,014,347 to Ballout ("the '347 patent")
Ex-1002	File History for U.S. Patent No. 12,014,347
Ex-1003	Declaration of Dr. Andrew Cockburn, Ph.D. ("Cockburn")
Ex-1004	Curriculum Vitae of Dr. Andrew Cockburn, Ph.D.
Ex-1005	U.S. Patent No. 8,195,576 to Grigg et al. ("*Grigg*")
Ex-1006	U.S. Patent Application Publication No. 2009/0152343 to Carter ("Carter")
Ex-1007	Google Security Blog, *Advanced sign-in security for your Google account*, https://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html (Feb. 10, 2011)
Ex-1008	U.S. Patent Application Publication No. 2012/0166554 to Preece
Ex-1009	U.S. Patent No. 8,971,819 to Nicoara et al.
Ex-1010	U.S. Patent No. 8,635,287 to Shih et al.
Ex-1011	International Appl. Publ. No. WO 02/28067 to Mathiassen
Ex-1012	U.S. Patent No. 3,466,394 to French
Ex-1013	U.S. Patent No. 8,732,855 to Thomas et al.
Ex-1014	U.S. Patent No. 8,819,150 to Osinga et al.
Ex-1015	*Authentication in an Internet Banking Environment*, Federal Financial Institutions Examination Council (Oct. 2005).
Ex-1016	U.S. Patent No. 7,373,515 to Owen
Ex-1017	U.S. Patent No. 7,657,489 to Stambaugh

Exhibit	Description
Ex-1018	Sugata Sanyal, et al., A Multifactor Secure Authentication System for Wireless Payment, *in* Emergent Web Intelligence: Advanced Information Retrieval, Advanced Information and Knowledge Processing (2010).
Ex-1019	Ali Al-Qayedi et al., *Combined Web/Mobile Authentication for Secure Web Access Control*, Wireless Communications and Networking Conference, Vol. 2 (Apr. 2004).
Ex-1020	File History for U.S. Patent No. 8,195,576 to Grigg
Ex-1021	Declaration of Mina Ching
Ex-1022	Mihai Hulea, *Fingerprint Recognition Distributed System*, 2008 IEEE International Conference on Automation, Quality and Testing, Robotics (May 2008)
Ex-1023	Shaun Whitehead, *IN SAFE HANDS: A review of mobile phone anti-theft designs*, European Journal on Criminal Policy and Research (Mar. 2008).
Ex-1024	Engadget, *Stick 'em up. A Pantech GI100? Then gimme your phone and your thumbs!*, https://www.engadget.com/2004-08-03-stick-em-up-a-pantech-gi100-then-gimme-your-phone-and-your.html
Ex-1025	Apple iPhone 4 Specifications, GSMArena, https://www.gsmarena.com/apple_iphone_4-3275.php.
Ex-1026	Newton 2.0 User Interface Guidelines for the Apple Newton MessagePad (1996).
Ex-1027	European Patent Publication No. EP0969644 to Tuomela
Ex-1028	Motorola Atrix 4G User's Guide (2011)
Ex-1029	Adrian Pocovnicu, *Biometric Security for Cell Phones*, Informatica Economică, vol. 13 (Jan. 2009).

LIST OF CLAIMS

[1pre]	A method of securely accessing a local application on a mobile device, comprising the steps of:
[1a]	launching a local application on a mobile device;
[1b]	enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application;
[1c]	launching the local application after the setting of the desired security level configuration setting; and
[1d]	requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels.
2	The method of claim 1, wherein the single security level scan includes a request for a password.
3	The method of claim 1, wherein the plurality of security level scans includes a biometric scan.
4	The method of claim 3, wherein the biometric scan includes a voiceprint.
5	The method of claim 3, wherein the biometric scan includes a thumbprint.

[6pre]	A system for securely accessing a local application on a mobile device, comprising the steps of:
[6a]	a hardware processor on a mobile device; and
[6b]	a local application on the mobile device and configured to be executed by the hardware processor;
[6c]	the local application including a first interface enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application,
[6d]	the local application including a second interface requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels.
7	The system of claim 6, wherein the single security level scan includes a request for a password.
8	The system of claim 6, wherein the plurality of security level scans includes a biometric scan.
9	The system of claim 8, wherein the biometric scan includes a voiceprint.
10	The system of claim 8, wherein the biometric scan includes a thumbprint.

I. PRELIMINARY STATEMENT

Petitioner Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc. (collectively, "Samsung"), requests *inter partes* review of U.S. Patent No. 12,014,347 (Ex-1001) and cancellation of claims 1-10.

The claims of the '347 patent recite "securely accessing a local application on a mobile device" and enabling a user to "set a desired security level configuration setting" that requires either a single or multiple "security level scans" before accessing a "feature" of the application. This is nothing more than allowing a user to enable multi-factor authentication before accessing a mobile application, which was well known and understood before the '347 patent's earliest claimed priority date of July 18, 2011. So too were interfaces for configuring mobile applications.

The prior art in this Petition leaves no doubt the claims are unpatentable. *Grigg* (Ex-1005) discloses authenticating a mobile device user during a transaction where the user chooses a "level" or "tier[]" of security. *See, e.g.*, *Grigg*, 2:50-64, 6:37-61, 8:38-41, 11:16-23, 14:63-66. *Grigg* discloses requesting authentication of the user's identity by "receiving input of ***at least one*** of a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan," *Grigg*, 21:58-62 (claim 13)[1], and provides an interface indicating multiple authentication methods are "ACTIVE," *Grigg*, Fig. 9. *Grigg* also discloses performing authentications by different users before authorizing a transaction. *Grigg*, 6:49-61. *Grigg* therefore anticipates claims 1-10. *Grigg* alternatively renders claims 1-10 obvious.

Like *Grigg*, *Carter* (Ex-1006) discloses authenticating a mobile device user during a transaction and describes nearly identical authentication methods as *Grigg*. *Carter* ¶¶[0005]-[0008]. *Carter* discloses using multi-factor authentication, particularly for high value transactions, *Carter* ¶[0031], including different authentication "levels" where "greater authentication can be required for higher value (and higher risk) purchases," and "each increasing level of authentication ***may cumulatively require*** authentication by all of the methods of each lower level in the hierarchy." *Carter* ¶[0032]. A POSITA would have combined *Grigg* with *Carter* to incorporate *Carter*'s multi-factor authentication and cumulative authentication scans, thus fulfilling *Carter*'s goal of increasing security and reducing fraud in financial transactions. *See Carter* ¶¶[0031]-[0032].

---

[1] All emphasis in quotations and color and colored annotations in figures have been added.

Removing all doubt, *Google* (Ex-1007) discloses interfaces for enabling two-factor authentication before permitting access to features on mobile devices. *Google*, 1. This includes interfaces for opting in (or not) to two-factor authentication before accessing Google features through a web browser. *Id.*

The Board should institute review and cancel all challenged claims.

II. STATE OF THE ART

Multi-factor authentication was known in the art before the ’347 patent. Cockburn ¶40. Such authentication requires two or more “factors,” such as something the user knows (e.g., password, PIN, etc.), something the user has (e.g., ATM card, smart card, token generator, etc.), and something the user is (e.g., biometric characteristic, such as a fingerprint, etc.). Cockburn ¶40; Ex-1015, 3; Ex-1016, 2:21-24; Ex-1017, 1:54-64.

As early as 2005, the federal government was recommending multi-factor authentication for “high-risk transactions involving access to customer information or the movement of funds to other parties.” Ex-1015, 6. Before the ’347 patent, POSITAs understood that applying multi-factor authentication to authenticate mobile device users was well-known and understood. Cockburn ¶40; Ex-1018, Abstract (multi-factor authentication for “wireless based online payment applications”), 344-349; Ex-1019, 1 (systems for “augmenting the traditional Web-based username/ password approach with a Mobile-based challenge/response authentication”).

Interfaces for setting mobile application settings, including security settings, were also well known. Cockburn ¶¶40-41. In early 2011, for example, Motorola released the Android ATRIX 4G smartphone that featured a fingerprint reader for authentication and security. Cockburn ¶¶40-41; Ex-1028, 1. The ATRIX 4G provided a user interface with user checkboxes for customizing alternative authentication methods, including drawing a pattern, entering a PIN, entering a password, and using a fingerprint. Ex-1028, 60-62. Biometric methods for authenticating mobile devices users was also well known well before the ’347 patent. Cockburn ¶¶40-41; Ex-1029, Title, 61-63.

As demonstrated below, providing an interface for a user to set the type of authentication required for a mobile application, including choosing between single and multi-factor authentication, was not an advance over the prior art. Cockburn ¶¶40-41.

III. THE ’347 PATENT

The ’347 patent discloses method 300 for “setting up and activating a user mobile device (or station) 105, for use with the mobile transaction platform 200.” Ex-1001, 10:26-31.

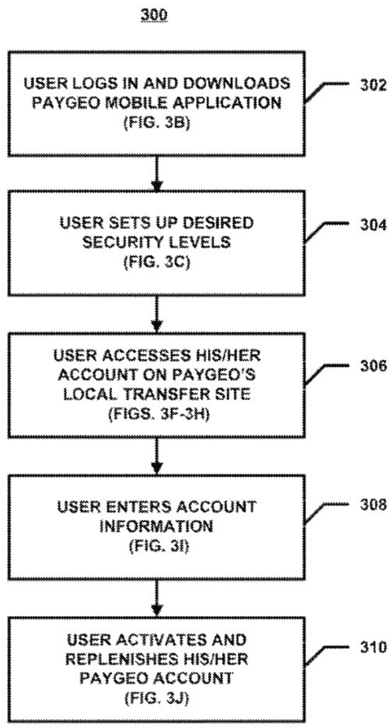


FIG. 3A

Ex-1001, Fig. 3A.

After downloading and starting a mobile application, a user may "set[] up the desired security level or levels for the user station 105." Ex-1001, 4:15-23, 10:32-39. The user may set "at least one of four security levels," including a first security level set by "entering a user-selected password," "recording a voice recognition password, signature, or template," "entering a user-selected fingerprint," and "providing a user DNA sample." Ex-1001, 10:40-53. The user may also elect "to enter alternative or additional security levels … , such as a thumb print 348 or a voice print 350." Ex-1001, 11:26-41. The user may then log into the application by "select[ing] the preferred identification 30 security levels that were previously set up at step 304." Ex-1001, 11:26-41.

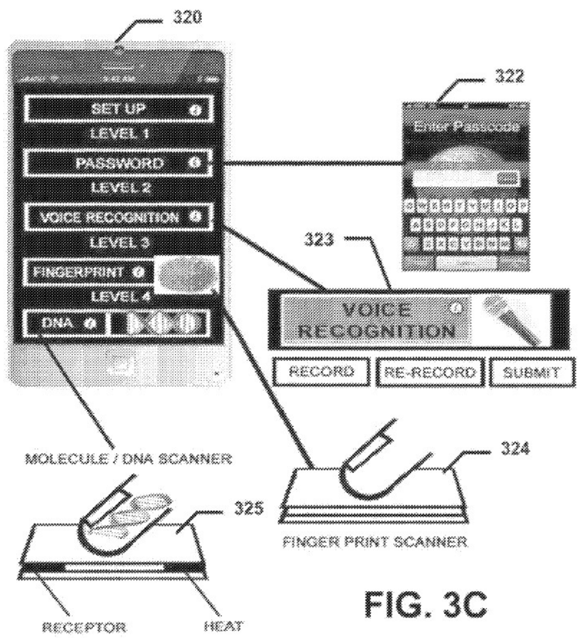


FIG. 3C

Ex-1001, Fig. 3C.

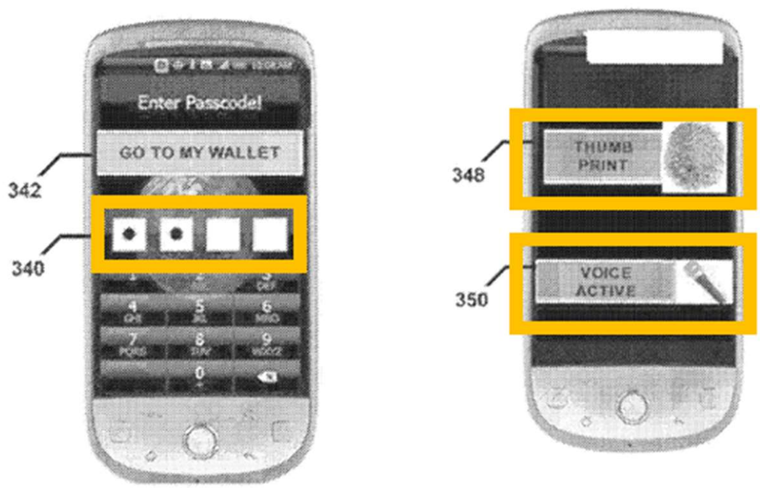


FIG. 3F FIG. 3H

Ex-1001, Figs. 3F, 3H (annotated); Cockburn ¶¶43-47.

IV. CLAIM CONSTRUCTION

The Board construes claims per *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b). Claims are construed only to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Here, no terms need construction to resolve the controversy in this forum.[2]

V. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art ("POSITA") would have had at least a bachelor's degree in electrical engineering, computer science, or a similar field and two years of experience designing graphical user interfaces, including those for mobile devices. Cockburn ¶¶52-54. Additional relevant work experience can compensate for less education, and vice versa. *Id.*

[2] Petitioner reserves the right to argue in an appropriate forum that certain limitations in the challenged claims are indefinite and/or lack written description support.

VI. STATEMENT OF PRECISE RELIEF REQUESTED

A. Prior Art

U.S. Patent No. 8,195,576 ("*Grigg*," Ex-1005), was filed on January 31, 2011, and issued on June 5, 2012, and is prior art to the '347 patent under 35 U.S.C. § 102(a)(2).[3]

U.S. Patent Application Publication No. 2009/0152343 ("*Carter*," Ex-1006), published on June 18, 2009, and is prior art to the '347 patent under 35 U.S.C. § 102(a)(1).[4]

Google's "*Advanced sign-in security for your Google account*" is an online blog article (Ex-1007) that posted on February 10, 2011.

A copy of *Google* was archived by the Internet Archive the day *Google* posted (February 10, 2011). Ex-1021 ¶¶1-7; *see also* Ex-1021, Ex. A (showing *Google* was archived on "20110210192241," corresponding to February 10, 2011, at 7:22 PM and 41 seconds). *Google* was therefore publicly available and

[3] The '347 patent includes a continuation-in-part application that was filed after the AIA transition date, making the '347 patent an AIA patent. To the extent the '347 patent is determined to be a pre-AIA patent, *Grigg* is prior art under pre-AIA 35 U.S.C. § 102(e).

[4] *Carter* is alternatively prior art under pre-AIA 35 U.S.C. § 102(b).

accessible to POSITAs via the Internet by this date. *See* Ex-1021 ¶¶1-7. *Google* is prior art to the '347 patent under 35 U.S.C. § 102(a)(1).[5] *See Dr. Squatch, LLC v. The Proctor & Gamble Co.*, IPR2024-01105, Paper 12 at 5-6, 18, 20, 26-29 (P.T.A.B. Jan. 27, 2025) (granting institution based on "a website advertising a deodorant product" deemed a printed publication based on the Wayback Machine archives).

B. Challenges

Ground	Challenged Claims	Basis	Prior Art
1A	1-10	§102	*Grigg*
1B	1-10	§103	*Grigg*
2	1-10	§103	*Grigg* and *Carter*
3A	1, 2, 6, 7	§102	*Google*
3B	1, 2, 6, 7	§103	*Google*
4	3-5, 8-10	§103	*Google* and *Carter*

[5] Google is alternatively prior art under pre-AIA 35 U.S.C. § 102(a).

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Grounds 1A and 1B: Claims 1-10 Are Anticipated and/or Rendered Obvious by *Grigg*

1. Overview of *Grigg*

Grigg discloses a mobile transaction device security system in the form of a mobile device or "mobile wallet" that determines a "level" or "tier[]" of security before permitting a transaction. *Grigg*, Abstract, 1:48-3:41, 4:48-6:13, 6:37-61, 8:38-41, 11:16-23, 14:63-66. *Grigg* stores a security protocol based on user "instructions." *E.g.*, *Grigg*, 6:17-2, 6:37-61. The system determines when a user is engaging in a transaction and determines the necessary authentication. *E.g.*, *Grigg*, 9:32-10:11. *Grigg*'s mobile device receives input to authenticate the user by "receiving input of ***at least one*** of a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan." *Grigg*, 21:58-62 (claim 13); *see also Grigg*, 2:50-64. *Grigg* also discloses that authentication may be required by more than one user before permitting a financial transaction. *Grigg*, 6:51-53.

Grigg discloses exemplary user interfaces for establishing its authentication methods. Interface 900, for example, provides "an interface for viewing and editing security features capable of authenticating a user's identity." *Grigg*, 18:17-50, Fig. 9. This includes a "User Authentication tab 902" that identifies "the types of security features 906 that are uploaded to the financial transaction security system for that user." *Grigg*, 18:17-50, Fig. 9. Interface 900 enables a user to "edit 914 the stored features using the mobile device" and indicates which of the authentication methods are "ACTIVE" or not. *Grigg*, 18:17-50, Fig. 9.

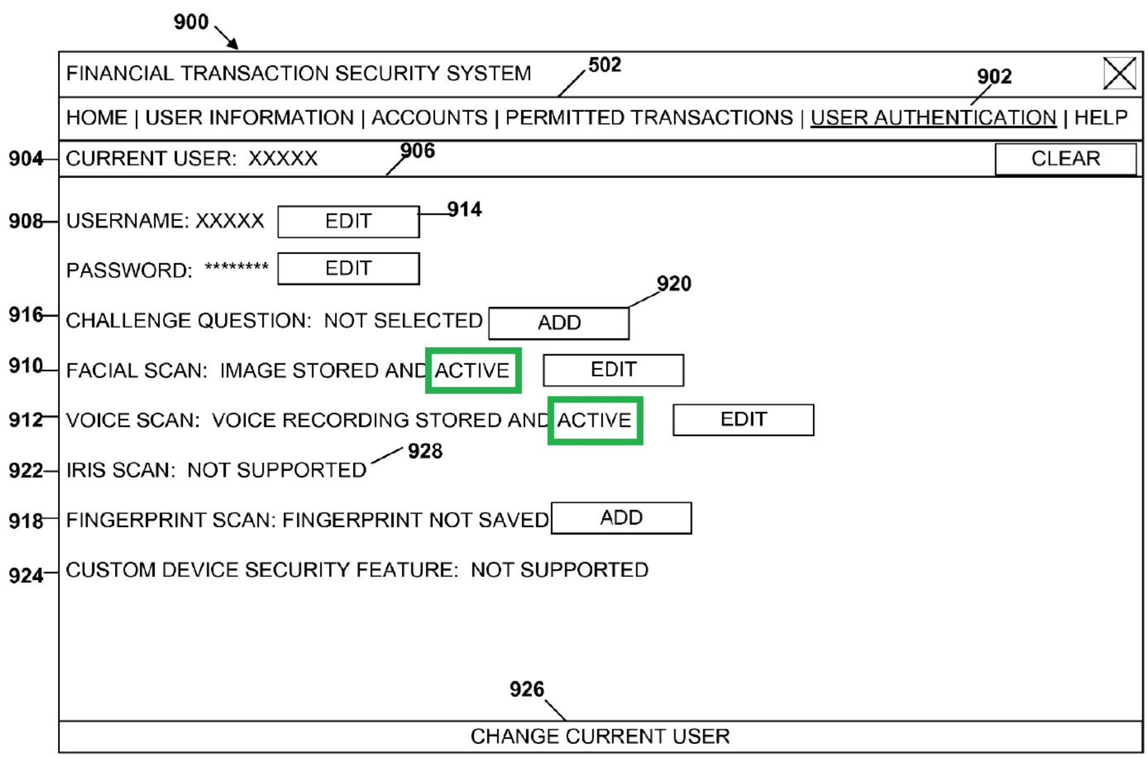


FIG. 9

Grigg, Fig. 9 (annotating "**ACTIVE**" authentication methods); Cockburn ¶¶55-60.

Grigg and the '347 patent are from the same field of endeavor: application security to protect a user's sensitive information. Cockburn ¶60. *Grigg* seeks to improve the security of applications (e.g., its mobile wallet) by providing interfaces that allow a user to protect sensitive information by requiring authentication during a transaction by user password and/or biometric information. *Grigg*, 1:57-60, 2:4-7, 10:66-11:23. The '347 patent is similarly directed to user interfaces for securing a mobile application by enabling a user to require authentication that may include a password and biometric information. Ex-1001, Abstract, 10:32-53, 11:26-41. *Grigg* is therefore analogous art to the '347 patent. Cockburn ¶60.

2. Independent Claim 1

a. [1pre]: "A method of securely accessing a local application on a mobile device, comprising the steps of:"

Grigg discloses a method of securely accessing a local application on a mobile device. Cockburn ¶¶75-84.

Mobile device: *Grigg* refers to its mobile device as a "mobile wallet," "electronic wallet," or "financial transaction security system." *Grigg*, 1:48-3:41, 3:54-67, 4:48-52, 10:58-61, 12:35-15:42, 15:44-18:50. Embodiments include "an electronic mobile device (e.g., a cell phone, personal data assistant, mp3 player, handheld computer, etc.) that is configured to be used as a payment device (such as a credit or debit card)." *Grigg*, 1:57-2:3; *see also Grigg*, 3:14-26, 12:35-49.

The mobile wallet "stores payment information in its memory that can be used to identify one or more financial accounts," and allows "people [to] use their mobile phones or similar mobile devices to engage in financial transactions."

Grigg, 1:57-2:3, 1:25-34. This includes "communicat[ing] payment information to [a point-of-sale or] POS terminal." *Grigg*, 1:25-34, 1:57-2:3.

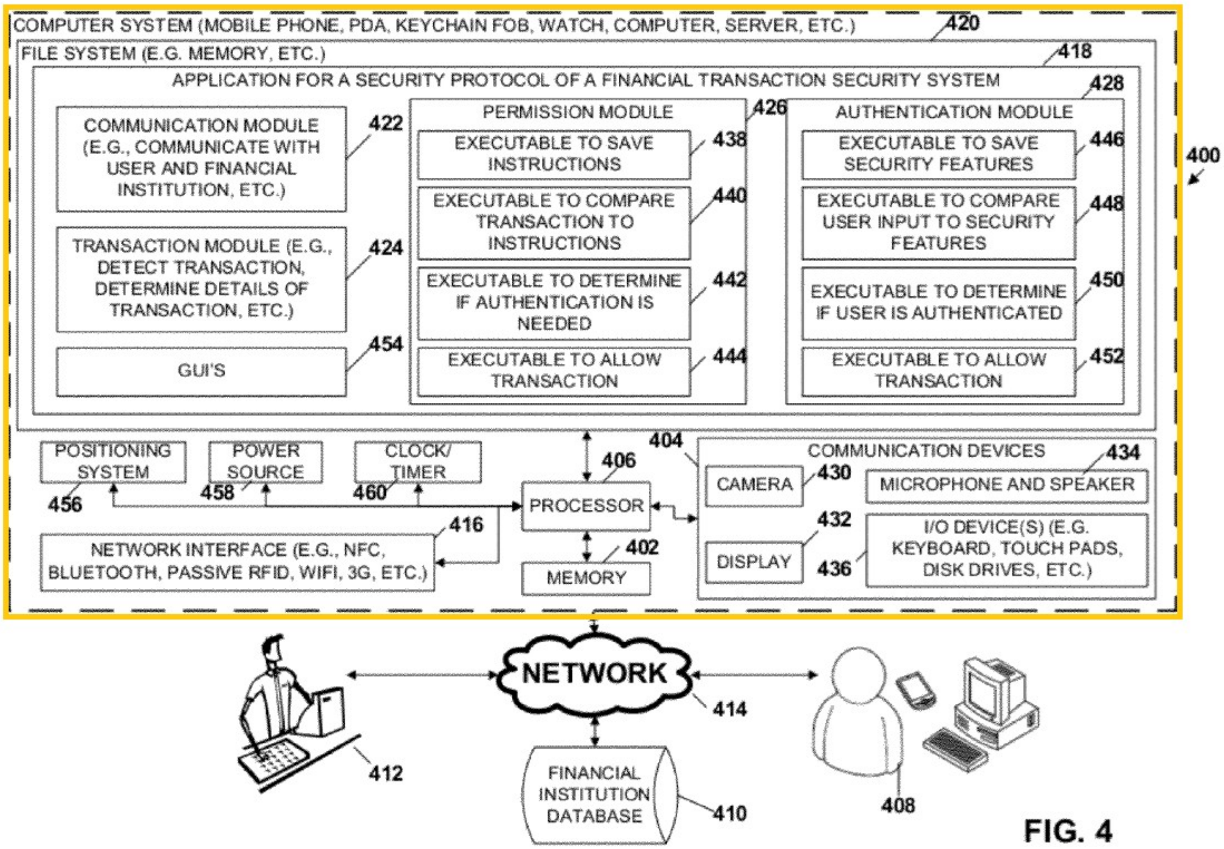


FIG. 4

Grigg, Fig. 4 (annotating system 400), 12:35-40 ("In some embodiments, the system 400 includes a computer system such as a mobile phone, PDA, keychain fobs, watch, computer, server, electronic device, etc."); Cockburn ¶77.

Grigg's financial transaction security system, which may be a mobile phone, smartphone, PDA or the like, is a "mobile device," as claimed. Cockburn ¶¶76-78.

Local application on the mobile device: A user in *Grigg* may "enter[] [a] security protocol into an interface on a mobile device application, a software program, or a webpage." *Grigg*, 4:48-64; *see also Grigg*, 3:27-41 (describing "an application on a smartphone … stor[ing] the user's security protocol"), 6:14-28 (receiving the security protocol "through a software application"). *Grigg* thus discloses a "local application" on its mobile device. Cockburn ¶¶79-83.

Grigg's mobile device application, or "security protocol application 418," includes a permission module 426 and an authentication module 428. *Grigg*, 13:11-65, Fig. 4. The security protocol application 418 can "receive[] and store information related to the financial transaction security system . . . and authenticate the user's identity." *Grigg*, 13:16-24. The application 418 includes "Graphical User Interfaces (GUI's) 454" that assist the user in "utilizing … any … feature of the … system 400." *Grigg*, 15:15-23, Fig. 4.

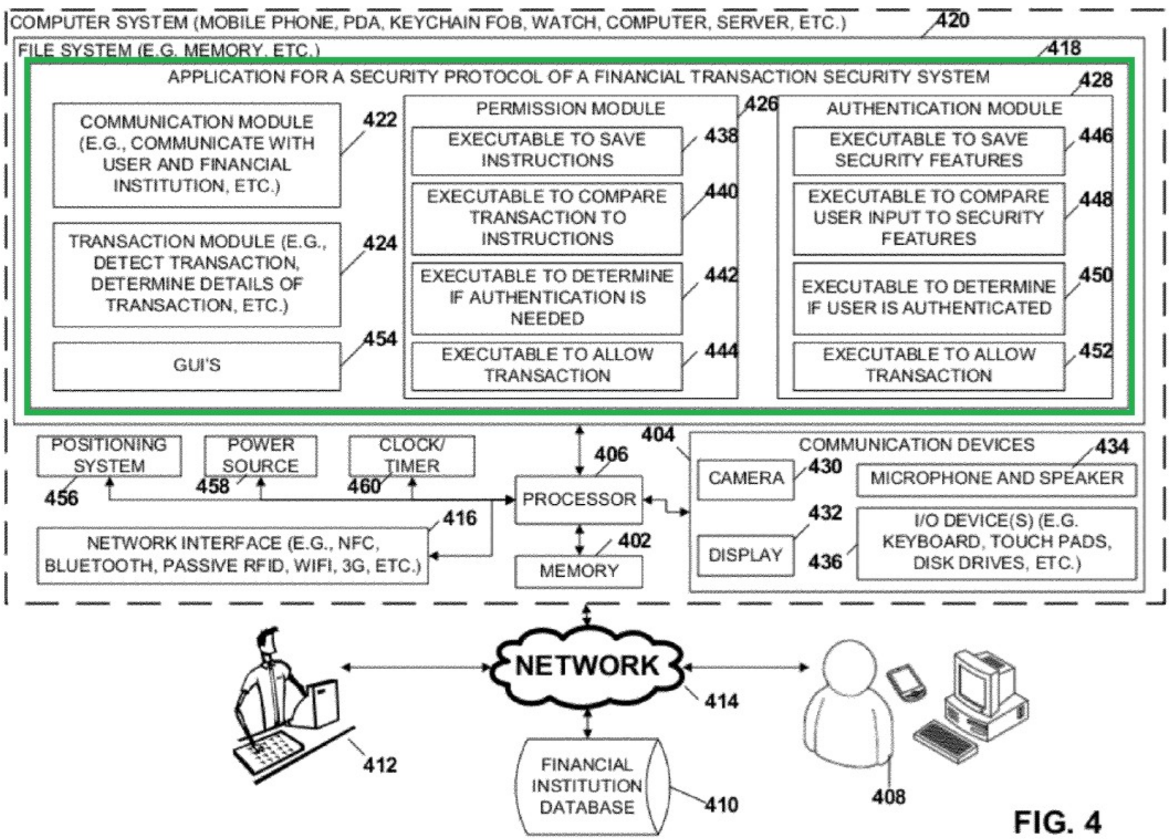


FIG. 4

Grigg, Fig. 4 (annotating **security protocol application 418**); Cockburn ¶80.

A POSITA would have understood *Grigg*'s security protocol application 418 is the same mobile device application referenced throughout *Grigg*, including Figures 1-3. Cockburn ¶¶81-83. In each of these embodiments, *Grigg* describes the application as receiving a security protocol from a user. *Grigg*, 2:65-3:41, 4:48-63, 6:21-28, 13:11-24. *Grigg* also explains that the security protocol application 418 is "the embodiment illustrated in FIG. 4 and described throughout much of this specification." *Grigg*, 13:11-24.

Grigg's mobile device application for entering a security protocol, including security protocol application 418, is a "local application on a mobile device," as claimed. Cockburn ¶¶79-83.

Securely accessing the local application on the mobile device: As discussed below, *Grigg* discloses a method of securely accessing its mobile device application, including security protocol application 418, to enable authenticating a user during a transaction. *See* Element [1d]; *see Grigg*, Abstract, 1:48-3:41, 4:48-6:13 (describing Fig. 1), 6:14-10:57 (describing Fig. 2), 10:58-12:34 (describing Fig. 3), Figs. 1-3.

Grigg thus discloses "[a] method of securely accessing" the local application on the mobile device, as claimed. Cockburn ¶¶84-85.

b. [1a]: "launching a local application on a mobile device;"

Grigg discloses Element [1a]. Cockburn ¶¶86-89. For example, as discussed for Element [1pre], *Grigg*'s mobile device application, including security protocol application 418, is a local application on the mobile device. *Id.*

To enter *Grigg*'s security protocol, "the user ***may initiate [the] application*** on a mobile phone and then enter details relating to the security protocol ***into the application***." *Grigg*, 4:53-58. The "application" being initiated in this example is *Grigg*'s mobile device application or security protocol application 418, as *Grigg* explains that this application is configured to receive the security protocol and authenticate a user based on a security protocol at a point-of-sale location. Cockburn ¶88; *Grigg*, 4:48-64; 6:14-28, 13:11-24.

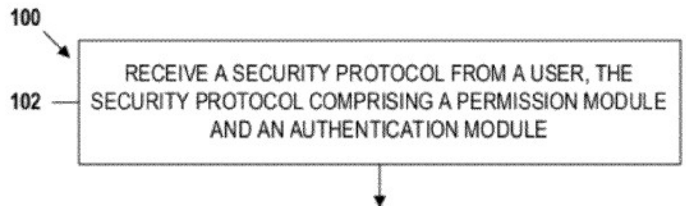
Grigg therefore discloses "launching" a local application on the mobile device. Cockburn ¶¶86-89.

c. [1b]: "enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application;"

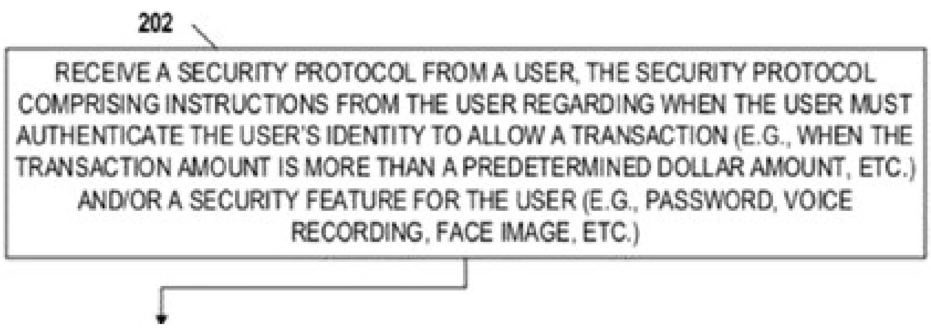
Grigg discloses or at a minimum renders obvious Element [1b]. Cockburn ¶¶90-128.

Enabling a user to set a desired security level configuration setting in the local application for the mobile device: *Grigg*'s mobile device application, including security protocol application 418, enables a user to customize "security protocols" for transactions. *Grigg*, 1:57-60, 2:4-7, 3:10-14, 3:27-32. For example, "the financial transaction security system 100 receives a security protocol from a user 102," where the user "enters the security protocol into an interface on a mobile device application." *Grigg*, 4:48-63. The security protocol is "customizable by the user." *Grigg*, 4:48-63; *see also Grigg*, 5:29-31 (describing a "customizable set of security protocols"), 2:46-49 (same), 3:10-12 (same), 8:31-41 (same), 8:49-

55 (same), 16:63-65 (same). Figures 1 and 2 illustrate receipt of the user's chosen method(s) of authentication by *Grigg*'s system:



Grigg, Fig. 1 (cropped).



Grigg, Fig. 2 (cropped).

Grigg discloses that its security protocol "is saved in a mobile device of the user." *Grigg*, 8:55-9:11. The mobile device further includes an authentication module that "includes the security features provided by the user as well as any hardware and/or software used to compare an input from the user to those security features." *Grigg*, 4:64-5:11. Before enabling the user to perform a transaction, the system compares input from the user, such as a voice command, facial scan, etc., to the security features of the security protocol "saved by the user as part of the authentication module." *Grigg*, 5:60-6:7; *see also Grigg*, 10:58-11:32, 11:43-12:25, 13:16-24, Figs. 3, 4. Claim 13 of *Grigg* discloses "requesting authentication of the user's identity comprises receiving input of ***at least one of*** a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan." *Grigg*, 21:58-62.[6] *Grigg* thus discloses authenticating a user by one or more authentication methods. Cockburn ¶¶91-98. In one embodiment, the user may require authentication by two individuals. *Grigg*, 6:45-61. Indeed, *Grigg* discloses authenticating its user "in a variety of ways" based on the security features. *Grigg*, 10:66-11:23. An authentication request "allows a user to authenticate his identity in any manner" or "in a specific manner." *Grigg*, 10:66-11:23.

Grigg provides an exemplary interface for enabling a user to enter its security features. Cockburn ¶¶98-100. Figure 9 depicts an interface 900 "for viewing and editing security features capable of authenticating a user's identity in a financial transaction security system." *Grigg*, 18:17-50, Fig. 9. The interface allows entry of a username and password 908, a user's facial scan 910, a user's voice scan 912, a user's iris scan 922, a challenge question 916, and a user's fingerprint scan 918. *Grigg*, 18:17-50, Fig. 9. The user can configure the

[6] Claim 13 was originally filed as claim 20 with the application leading to *Grigg* and thus is part of *Grigg*'s original disclosure. Ex-1020, 214-220.

authentication module with "at least one security feature." *Grigg*, 6:21-23, 20:62-65 (claims 2-3).

As shown below, interface 900 shows at least two of seven potential authentication methods are concurrently active. Cockburn ¶100. The active authentication methods are facial scan 910 and voice scan 912, which are each shown as "ACTIVE." *Grigg*, Fig. 9; Cockburn ¶100. The other available (but not stored) methods are challenge question 916, iris scan 922, fingerprint scan, and custom device security feature 924. *Grigg*, 18:30-42, Fig. 9; Cockburn ¶100.

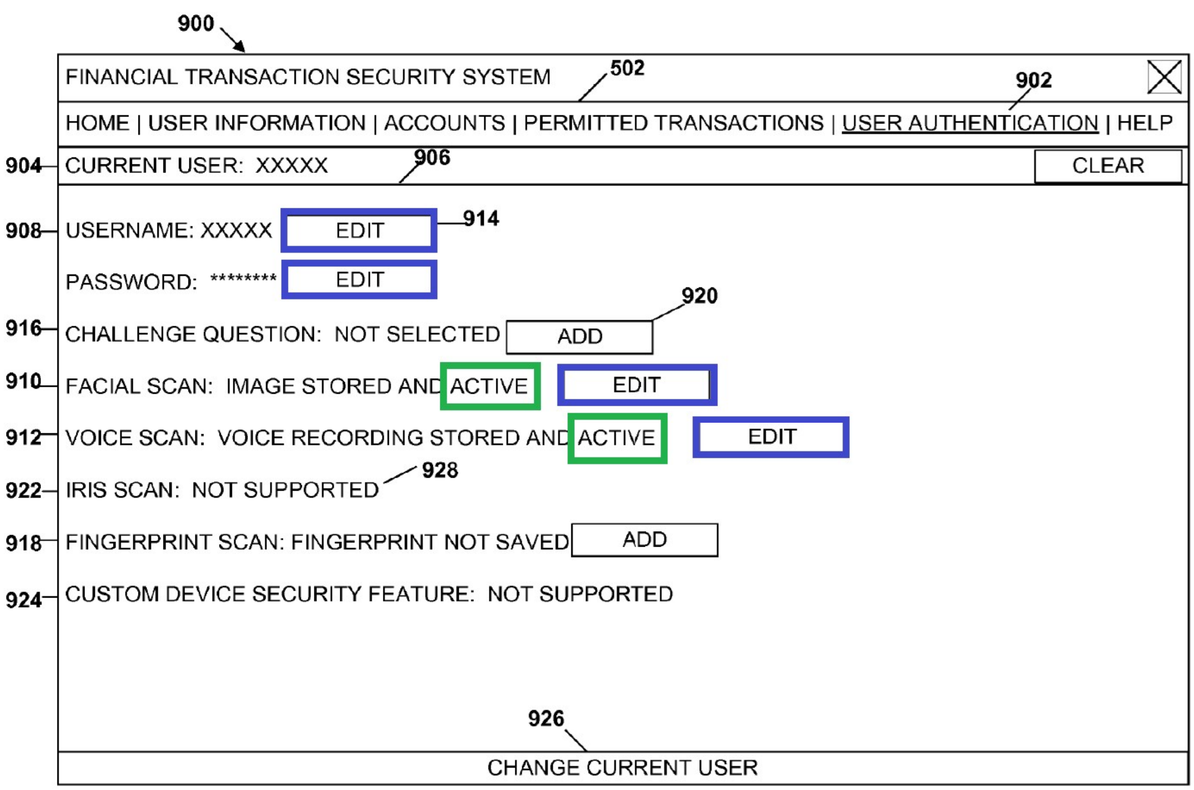


FIG. 9

Grigg, Fig. 9 (annotating the stored authentication methods a user can "**EDIT**" and those that are "**ACTIVE**").

A POSITA would have understood from *Grigg*'s disclosure of a user configuring a security module within security protocol application 418, including requiring authentication by a user by "at least one" security feature and indicating which features are "ACTIVE" via interface 900, discloses setting a desired security level configuration setting, as claimed. Cockburn ¶¶100-103.

The desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels: *Grigg* discloses or at least renders this feature obvious. Cockburn ¶¶104-125.

As discussed, *Grigg* discloses that the user can configure the authentication module with more than one security feature *Grigg*, 6:21-23, 20:62-65 (claims 2-3), 21:58-62; Cockburn ¶¶100-103. *Grigg* also discloses that authentication "can occur in a variety of ways," including in a "specific manner" as defined by the user. *Grigg*, 10:66-11:23. This includes setting "different ***tiers*** of authentication." *Grigg*, 10:66-11:23; *see also Grigg*, 7:56-60 (disclosing "***different levels of security***"), 8:31-41 (customizing "***security levels***"), 6:45-61 (disclosing "tiered levels"). *Grigg* also discloses receiving user input "of at least one" authentication method when requesting authentication of a user's identity. *Grigg*, 21:58-62 (claim 13); *see also*

Grigg, 6:45-61 (receiving "***different types of authentication*** or lack thereof"). *Grigg* further discloses requiring authentication in embodiments by multiple users. *Grigg*, 6:45-61. Grigg thus discloses enabling a user to set a "security level configuration setting" that establishes a "single" or a "plurality" of security levels before allowing access to at least a feature in the local application, as claimed. Cockburn ¶¶100-107.

To the extent *Grigg* does not expressly disclose this (it does), *Grigg* at least renders this obvious. Cockburn ¶¶108-125.

For example, it would have been obvious to modify *Grigg* to apply its different "tiers" or "levels" of authentication by allowing a user to select between a single and multiple "ACTIVE" security features and before authorizing a transaction. Cockburn ¶¶109-110.

A POSITA would have found it obvious to modify interface 900, for example, to enable a user to "edit 914 … stored [security] features using the mobile device" and separately enable them as "ACTIVE" them according to Figure 9. *See Grigg*, 18:17-30, Fig. 9; Cockburn ¶110. This would have allowed a user to save a username and password, an answer to a challenge question, and/or a user's biometric information via interface 900 and then activate one or more of those security features. Cockburn ¶111. This modification would have been an obvious based on *Grigg*'s own disclosure of storing multiple security features (e.g., password, facial recognition, fingerprint, etc.), enabling a user to implement the authentication module in a specific manner, setting "tiers" or "levels" of authentication based on transaction amounts, and its contemplated use of multiple authentication scans in exemplary embodiments (*see, e.g.*, *Grigg*, 6:51-53, 21:58-62). Cockburn ¶112.

A POSITA would have been motivated to modify *Grigg* in this way for several reasons. Cockburn ¶¶113-125.

For example, this modification would have enabled *Grigg* to load multiple security features and select which one (or more than one) of those security features are active before a transaction may proceed, giving the user flexibility in the implementation of *Grigg* and fulfilling its goal of being user-customizable and flexible. *See Grigg*, 3:10-14 (describing a system that "provides numerous opportunities for the user to customize security protocols relating to financial transactions conducted through mobile devices"), 1:48-56 (allowing users to "customize payment procedures and authentication protocols"), 2:46-49 (same), 5:29-31 (same), 8:31-41 (same), 8:49-55 (same); Cockburn ¶¶114-118.

As *Grigg* recognizes, a user may desire some transactions to have more security while convenience may be more important for others. *See, e.g.*, *Grigg*, 1:8-14 (desiring "both convenience and control over their transaction security"), 1:35-41 (same), 6:38-61 (requiring authentication above certain transaction amounts, including the option for dual approval by "couple[s]").

Allowing a user to select more than one active security feature would have improved the security of *Grigg*'s mobile wallet during a transaction. Cockburn ¶¶114-118. By allowing a user to require more than one authentication method (e.g., a password and biometric information) via interface 900, security at point-of-sale transactions would be improved by requiring certainty that the user is who he or she purports to be. *Id.* This would have reduced potential fraud by requiring multi-factor authentication using *Grigg*'s different security features, thus reducing the likelihood of unauthorized use of *Grigg*'s mobile wallet. *Id.*

This modification also would have fulfilled the desire to afford users convenience over security when desired, as *Grigg* contemplates. *See, e.g.*, *Grigg*, 1:8-14, 1:35-41, 6:38-61. For example, by allowing a user to require only a single user authentication method, e.g., a password, the transaction would proceed with "ease" and "speed." *See Grigg*, 8:42-55. This would have provided a user with the customization and control that Grigg contemplates. *See Grigg*, 1:8-14, 1:35-41, 1:48-56, 7:38-41, 8:18-55; Cockburn ¶¶114-118.

Applying multi-factor authentication to *Grigg*'s mobile wallet would have been well within the capabilities of a POSITA and involved nothing more than combining *Grigg*'s disclosed security features and multiple tiers or levels of security (including *Grigg* requiring "at least one" security feature) in understood ways. Cockburn ¶119. Indeed, *Grigg* suggests this by disclosing a user-configurable system that may be implemented "in a variety of ways" and a "specific manner" as defined by the user. *Grigg*, 10:66-11:23; Cockburn ¶119.

The modification also would have given a user greater clarity as to which security feature or features are active for a transaction when more than one are loaded and available. Cockburn ¶120.

A POSITA would have implemented this modification by either providing an option with interface 900's "edit 914" feature or by providing a selectable activation button by each loaded security. Cockburn ¶121.

Submenus and drill-down windows like this were well-known and ubiquitous at the time. *Id.* (citing Ex-1026, 46-49). *Grigg* such a menu via edit 914 of interface 900: "the user is able to edit 914 the stored features using the mobile device." *Grigg*, 18:17-50. It would have been obvious to provide an option within the menu of edit 914 that allows a user to activate a stored security feature as well as load it. Cockburn ¶¶121-122. Interface 900 would then reflect which security feature is "ACTIVE":

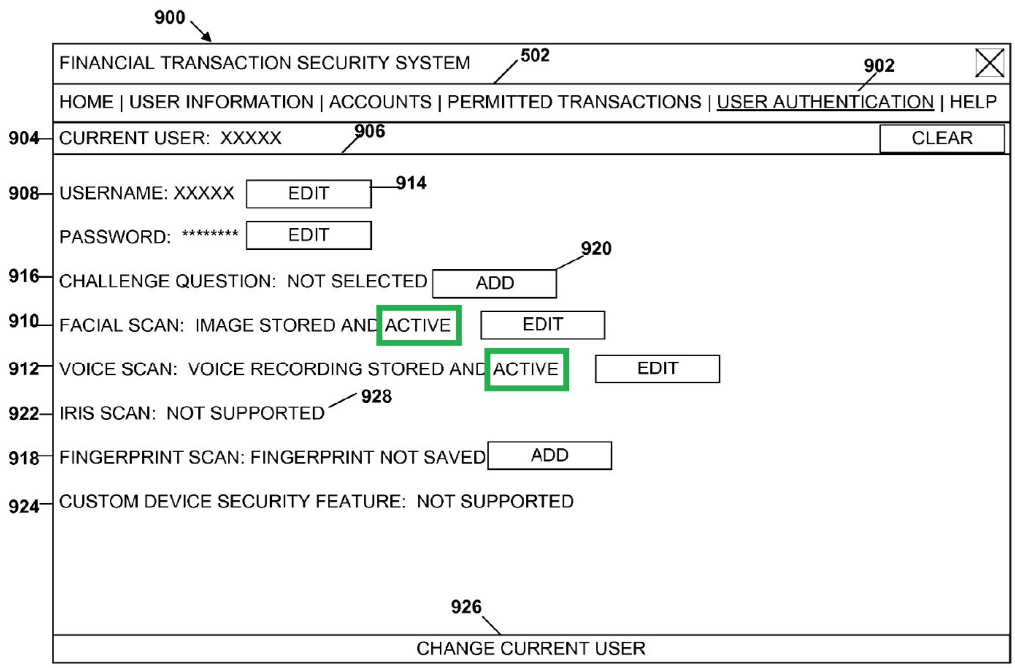


FIG. 9

Grigg, Fig. 9 (annotating "**ACTIVE**" security features); Cockburn ¶122.

Alternatively, it would have been obvious to modify *Grigg* to include an optional activation checkbox in interface 900 to select whether a security feature is active or not. Cockburn ¶¶123. Selectable GUI features like this were well-known and ubiquitous in user interfaces on mobile devices. *Id.* (citing Ex-1026, 112, 113).

As shown below in Figure 9, facial scan 910, voice scan 912, and user name and password 908 have loaded security features by virtue of their respective "EDIT" boxes being shown. *See Grigg*, Fig. 9; Cockburn ¶124. It would have been obvious to modify this interface to include an option to select which security feature is active by a selectable checkbox, as reflected below. Cockburn ¶124.

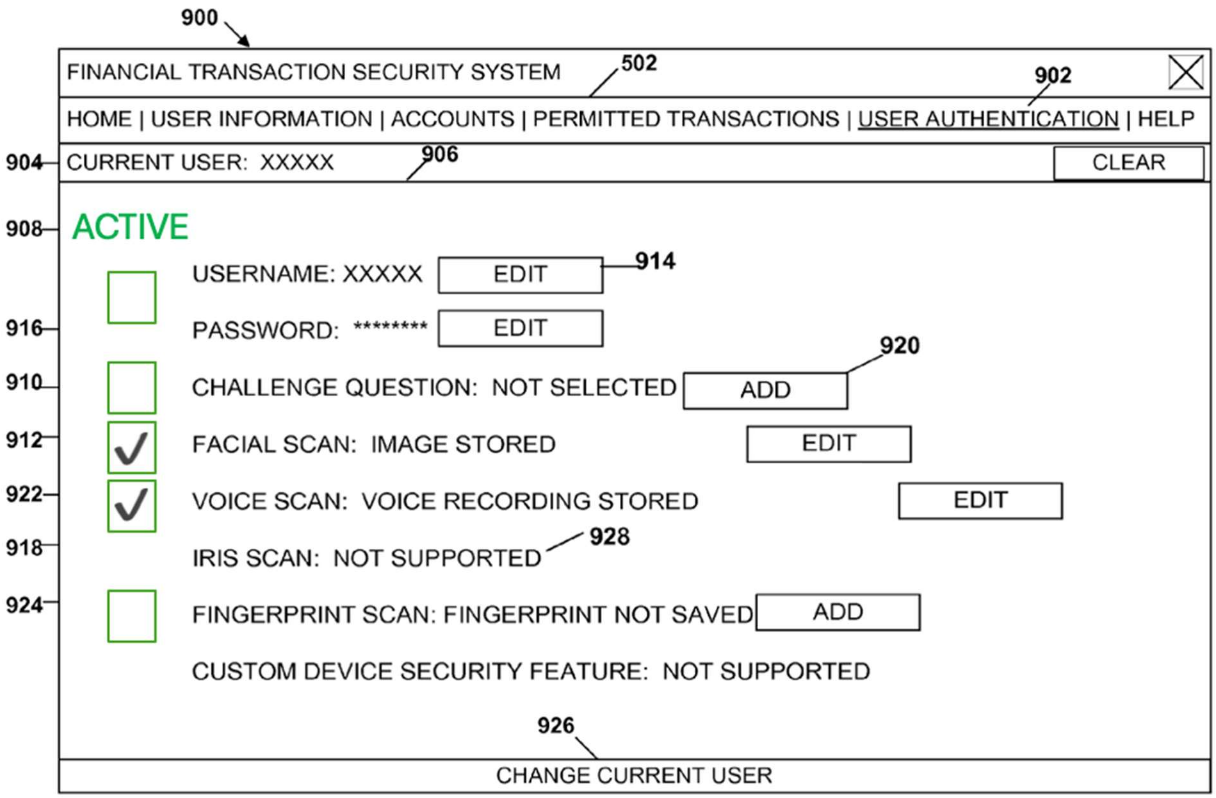


FIG. 9

Grigg, Fig. 9 (annotated with selectable **checkboxes** to activate or deactivate security features); Cockburn ¶124.

A POSITA would have had a reasonable expectation of success in either of these modifications because user selections such as these—either via a new edit window or via a checkbox—were well known and understood in the art. Cockburn ¶125 (citing Ex-1026, 46-69, 112, 113). This would have been well within a POSITA's capabilities and fulfilled *Grigg*'s disclosure that contemplates at least one authentication scan. *Id.* This also would have been consistent with *Grigg*'s emphasis on flexibility and user customization. *See Grigg*, 8:42-55; Cockburn ¶125.

<u>Before allowing access to at least a feature in the local application</u>: *Grigg* discloses that its authentication module compares user input to the stored security features to authenticate a user before permitting a transaction: "[i]f the user has successfully authenticated his identity, in some embodiments the system transfers the user's financial account information 316." *Grigg*, 12:26-34; *see also Grigg*, 10:50-57, 15:5-14. Allowing a transaction to proceed is a "feature" of *Grigg*'s security protocol application 418. Cockburn ¶¶126-127.

In *Grigg*, as expressly disclosed or modified, a transaction would be permitted after a user is authenticated based on entering a password, or entering a password and providing biometric information, depending on the activated security features. Cockburn ¶128. *Grigg* therefore discloses or at least renders obvious enabling a user to set a desired security level configuration setting establishing "whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application," as claimed. *Id.*

d. [1c]: "launching the local application after the setting of the desired security level configuration setting; and"

Grigg discloses Element [1d]. Cockburn ¶¶129-134. For example, *Grigg* discloses "activat[ing]" its mobile device application when conducting a transaction at a point-of-sale location. *Grigg*, 5:12-31. *Grigg* discloses that, after the security protocol is established, its mobile wallet determines that a user is conducting a transaction at a point-of-sale location. *Grigg*, 5:12-31, 9:32-42. To do so, "the user activates" the software application on the mobile device. *Grigg*, 5:12-31, 9:32-42. *Grigg* explains that transaction module 424—part of security protocol application 418—determines that the user is conducting a transaction and determines the details of the transaction." *Grigg*, 13:36-44; *see also Grigg*, 13:16-24.

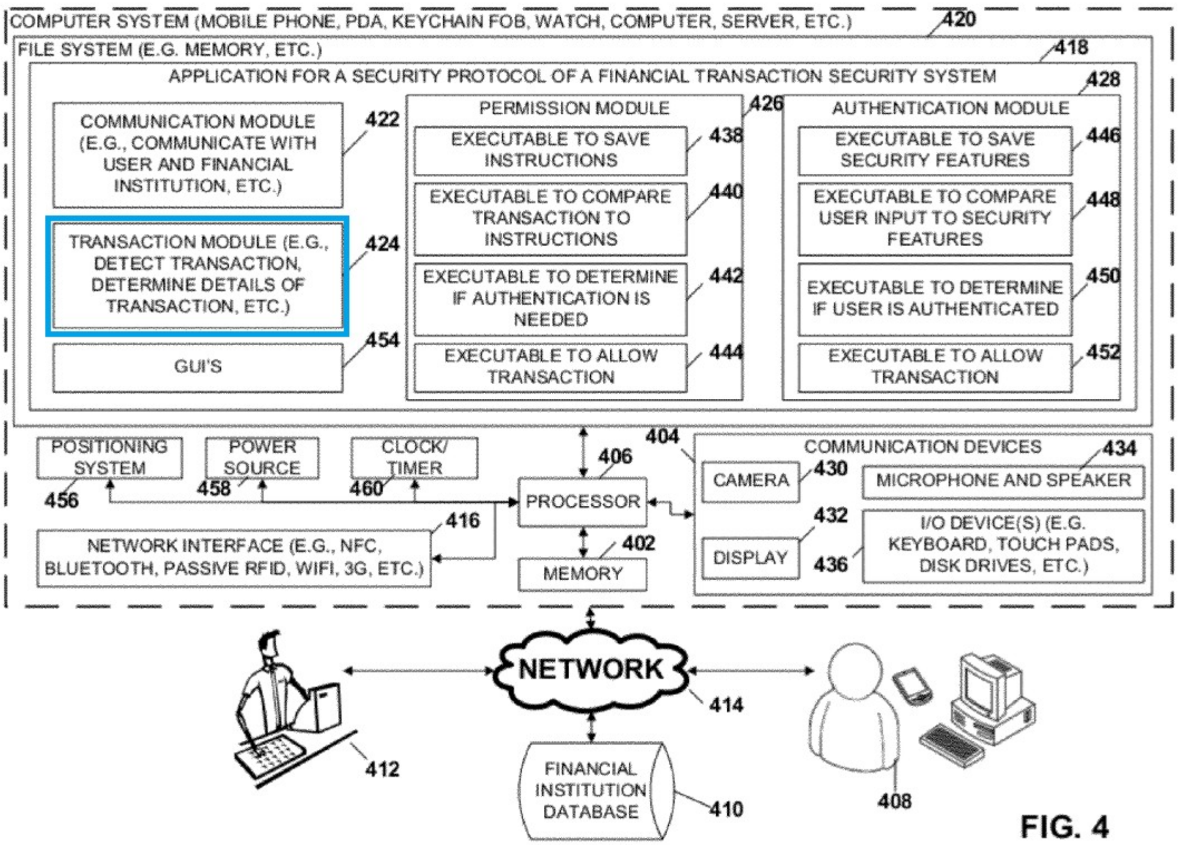


FIG. 4

Grigg, Fig. 4 (annotating **transaction module 424**); Cockburn ¶130.

Grigg's "activat[ing]" its mobile application, including security protocol application 418, to initiate a transaction at a point-of-sale location is "launching" the local application. Cockburn ¶¶129-131.

A POSITA would have understood that the same application in *Grigg* (e.g., security protocol application 418) is launched to set the desired security level configuration setting and is launched at a point-of-sale location to conduct a transaction after the desired security level configuration setting it set. Cockburn ¶132. Indeed, *Grigg* discloses comparing the transaction details to previous user input to the security protocol application 418 and then authenticating the user based on input to security protocol application 418 specifying the specific security features to use for a given transaction level. *See, e.g.*, *Grigg*, 5:60-6:7, 10:9-57, 11:55-12:19, 12:66-13:15:14; Cockburn ¶132. *Grigg* therefore discloses setting the desired security level configuration setting in the same application as used to conduct a later transaction because prior inputs to the same application are compared and used to authenticate a user during a transaction. Cockburn ¶133.

Grigg thus discloses Element [1c]. Cockburn ¶¶129-134.

e. [1d]: "requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels."

Grigg discloses "requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting," as claimed. Cockburn ¶¶135-146.

Grigg discloses or at least renders obvious the "authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels." Cockburn ¶136.

Requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting: As discussed for Element [1c], *Grigg*'s mobile device determines that a user is conducting a transaction at a point-of-sale location. *See* Element [1c]; *Grigg*, 5:12-31, 9:32-42, 13:36-44. Allowing a transaction to proceed by enabling payment to a merchant is a "feature" of *Grigg*'s mobile application. *See* Element [1b]; *Grigg*, 12:26-34; *see also Grigg*, 10:50-57, 15:5-14; Cockburn ¶137

Before a transaction may proceed, the mobile device compares "instructions" stored in a permission module to determine what user authentication (if any) is required for a given transaction. *Grigg*, 4:64-5:48. The device "compares the details of the transaction with the instructions regarding when the user must authenticate his identity." *Grigg*, 10:9-16, 10:44-57; *see also Grigg*, 5:32-59, 6:21-8:55 (describing various "instructions"). If a transaction requires authentication, the mobile device authenticates a user by comparing user input to stored security features. *Grigg*, 5:5-8, 5:60-6:8 (comparing "the voice command or the facial scan, for example, with security features saved by the user as part of the authentication module"), 10:62-12:19, 14:20-15:14.

Grigg therefore discloses requiring, before allowing access to the feature of the local application, the user to perform an authentication process based on the desired security level configuration setting. Cockburn ¶¶137-139.

The authentication process including only a single security level scan or a plurality of security level scans based on the desired security level configuration setting: *Grigg* discloses or at least renders this feature obvious. Cockburn ¶¶140-146.

For a single security level scan, *Grigg* discloses a user providing input in the form of a password and comparing that input to the stored security features to authenticate the user before allowing a transaction. *Grigg*, 5:5-8, 5:60-6:8, 10:62-12:19, 14:20-15:14; Cockburn ¶141.

For a plurality of security level scans, as discussed for Element [1b], *Grigg* discloses or at least renders this obvious; Cockburn ¶¶142-145.

For example, *Grigg* discloses authenticating a user by "receiving input of ***at least one of*** a username, a password, an answer to a challenge question, a voice recognition scan, a facial scan, a fingerprint scan, and an iris scan." *Grigg*, 21:58-62 (claim 13). *Grigg* also discloses that "a couple may decide that for transaction amounts greater than $200 ***authentication by both individuals is required***." *Grigg*, 6:45-61. Both of these embodiments disclose a plurality of security scans based on the security level configuration setting set by the user. Cockburn ¶142.

Alternatively, as discussed for Element [1b], it would have been obvious to modify *Grigg* to enable a user to select multiple "ACTIVE" security features before authorizing a transaction at a point-of-sale location. *See Grigg*, 18:22-30, Fig. 9; Cockburn ¶143. Modified *Grigg* renders obvious a plurality of security scans based on the security level configuration setting set by the user. Cockburn ¶143. Before allowing a transaction, a user would perform a single or multiple authentication steps based on the "ACTIVE" security features in interface 900. *See* Element [1b]; Cockburn ¶143.

As discussed for Element [1b], modifying *Grigg* in this manner would have been nothing more than combining known security features in *Grigg* in well-understood ways and, based on *Grigg*'s emphasis on flexibility, user customization, and security, require either a single or plurality of security level scans before a transaction may proceed. Cockburn ¶144; *Grigg*, 4:48-63 (describing a customizable set of security protocols), 5:29-31 (same), 3:10-12 (same), 8:42-55 (customizing security protocol), 16:63-65 (same), 10:66-11:23 (authenticating "in a variety of ways" as defined by the user).

A POSITA would have been motivated to modify *Grigg* in this way for the reasons discussed in Element [1b], including improving security of *Grigg*'s mobile wallet during a transaction, allowing flexibility for the user, and providing clarity as to which security features are enabled for a transaction. Cockburn ¶145; *see* Element [1b].

Grigg therefore discloses or at least renders Element [1d] obvious. Cockburn ¶¶140-146.

3. Claim 2

a. "The method of claim 1, wherein the single security level scan includes a request for a password."

Grigg discloses a single security level scan that includes a request for a password. Cockburn ¶¶147-150.

As discussed for Elements [1b] and [1d], *Grigg* discloses a single security level scan that includes authenticating a user by "user name and password." *See* Elements [1b], [1d]; *Grigg*, 2:50-64, 5:49-59, 6:45-51 (requiring "a user name and password"), 11:2-12:19 (same), 14:27-30 (same), 18:25-27 (same). This is further shown below:

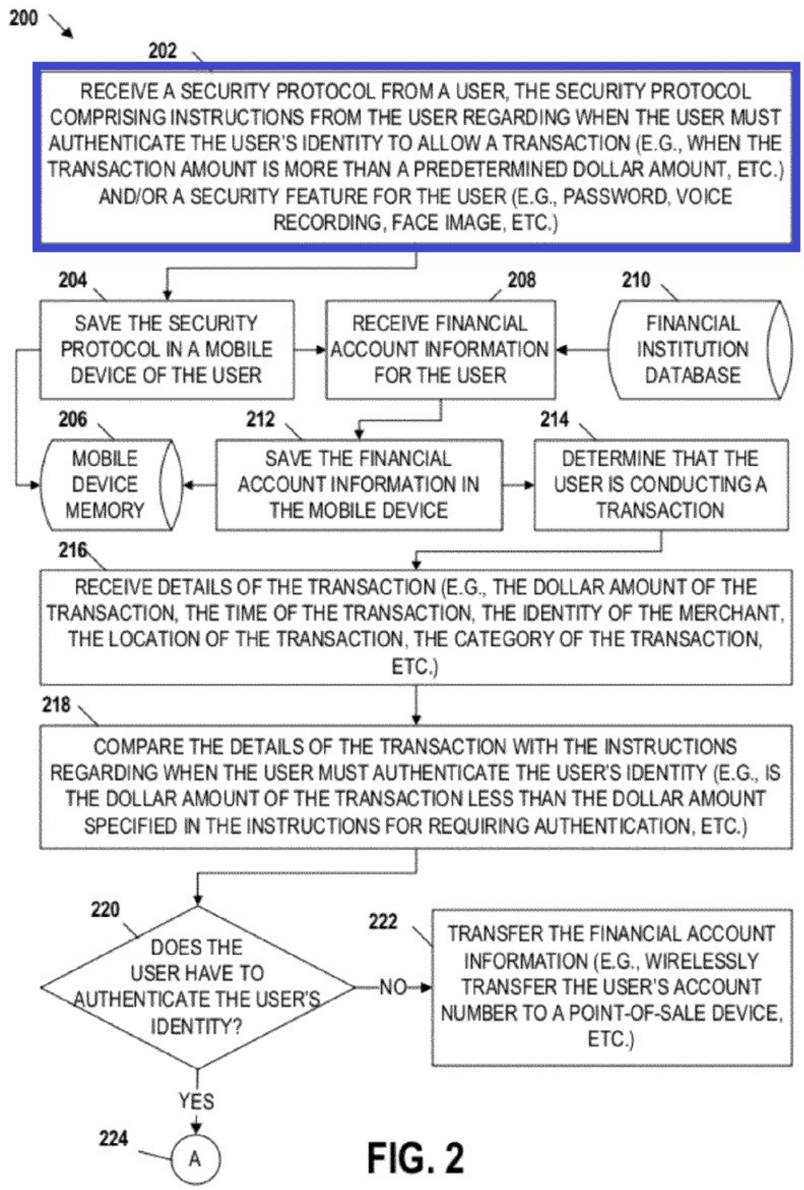


FIG. 2

Grigg, Fig. 2 (annotating **block 202**).

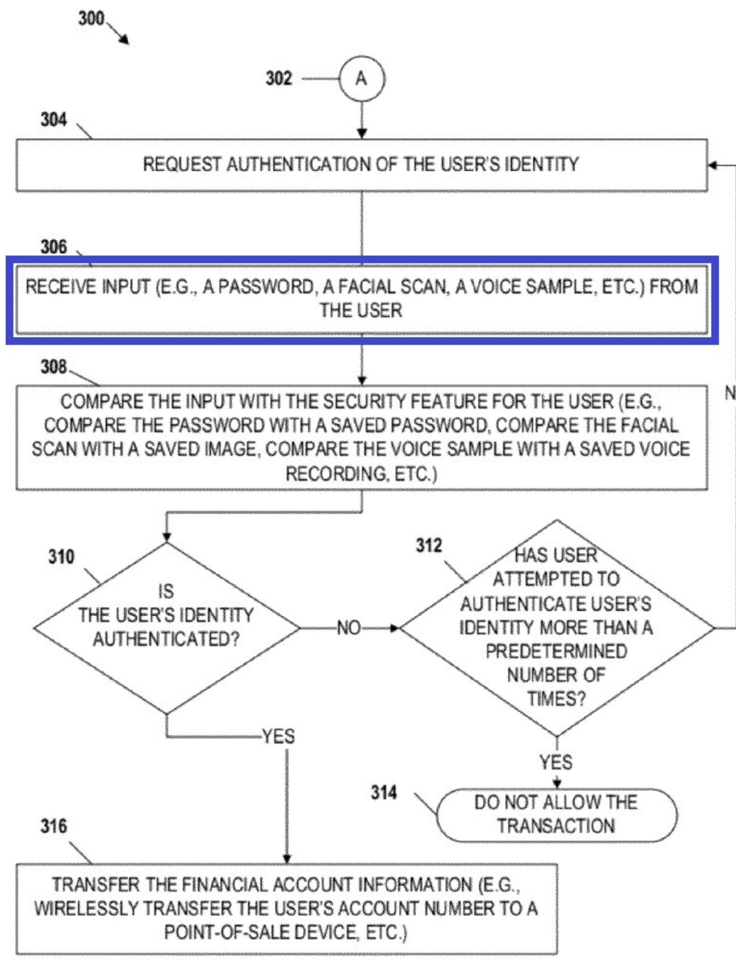


FIG. 3

Grigg, Fig. 3 (annotating **block 306**). *Grigg*'s requirement of a username and password is a single security level scan that "includes a request for a password." Cockburn ¶¶147-150.

Grigg therefore anticipates claim 2. Alternatively, in the modified *Grigg* system, a user would specify (e.g., via UI 900) a single activated security feature that includes *Grigg*'s username and password, which would at least render obvious claim 2. *Id.*; *see* Elements [1b], [1d].

4. Claim 3

a. "The method of claim 1, wherein the plurality of security level scans includes a biometric scan."

Grigg discloses or at least renders obvious a plurality of security level scans that "includes a biometric scan." Cockburn ¶¶151-154.

As discussed for Elements [1b] and [1d], *Grigg* discloses or at least renders obvious a plurality of security level scans. *See* Elements [1b], [1d]. *Grigg* discloses that its security features, as configured by the user, include a "biometric scan." *Grigg*, 6:45-61, 11:11-23. *Grigg*'s biometric scans include "a voice sample, a facial scan, a fingerprint scan, [and] an iris scan." *Grigg*, 2:54-59; *see also Grigg*, 11:24-32, 11:43-12:19, 14:52-15:4, 18:30-40, 20:66-21:2, 21:58-62. This is further shown in *Grigg*'s process flow below:

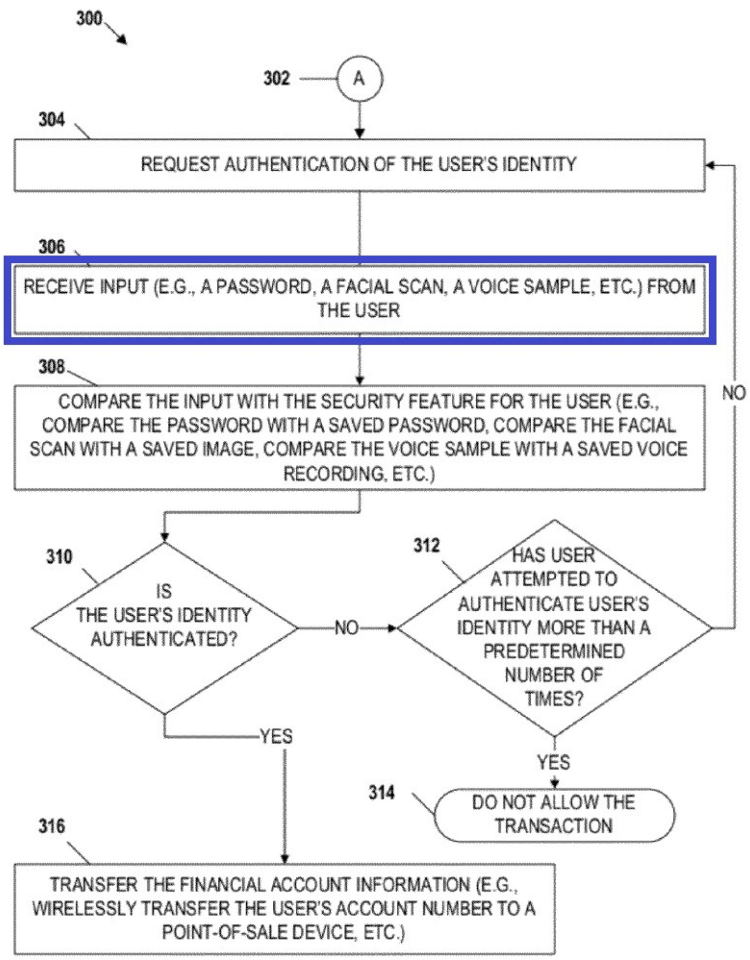


FIG. 3

Grigg, Fig. 3 (annotating **block 306**).

Grigg discloses—or alternatively as modified, would have included—a first single security level scan (e.g., that may include a request for a password) and one or more additional security level scans that include biometric information such as a voice sample, facial scan, fingerprint scan, and/or iris scan. Cockburn ¶¶151-154; *see* Elements [1b], [1d]. The user would provide input via the mobile device for comparison to the stored security features for authenticating the user before allowing the transaction. Cockburn ¶¶151-154; *see, e.g.*, *Grigg*, 2:50-64 ("The authentication module compares the input with the security feature to authenticate the identity of the user."), 3:28-41, 5:5-8, 5:60-6:7, 11:55-12:19, 14:20-15:14.

Grigg therefore discloses or at least renders obvious claim 3. Cockburn ¶¶151-154.

5. Claim 4

a. "The method of claim 3, wherein the biometric scan includes a voiceprint."

Grigg discloses the biometric scan includes a voiceprint. Cockburn ¶¶155-160.

As discussed for claim 3, *Grigg* discloses that its security features may include a "biometric scan." *Grigg*, 6:45-61, 11:11-23. *Grigg*'s biometric scan may include a "voice sample." *Grigg*, 2:54-59, 11:24-32, 11:43-12:19, 14:52-15:4, 18:30-40 ("voice scan 912"), 20:66-21:2, 21:58-62.

Grigg's mobile device "compare[s] … the voice sample with the saved voice recording" to authenticate a user before allowing a transaction. *Grigg*, 11:55-67, 11:24-32 (receiving voice sample via "a microphone … associated with the user's mobile device"); *see also Grigg*, 11:43-54, 12:20-25, 14:42-45; Cockburn ¶¶155-157.

A POSITA would have understood that *Grigg*'s "voice sample" is the claimed "voiceprint" because these synonymously describe a biometric identifier that is based on the characteristics of a person's voice. Cockburn ¶158. This is consistent with the '347 patent, which discloses using voice recognition to set "[t]he second security level." Ex-1001, 10:45-47 (describing setting the second security level "by recording a voice recognition password").

Grigg discloses—or alternatively as modified, would have included—a first single security level scan (e.g., that may include a request for a password) and one or more additional security level scans that include biometric information such as a voice sample. Cockburn ¶159; *see* Elements [1b], [1d]. The user would provide voice input via the mobile device for comparison to the stored security features (e.g., a stored voice recording) for authenticating the user before allowing the transaction at the point-of-sale location. Cockburn ¶159; *see, e.g.*, *Grigg*, 2:50-64, 3:28-41, 5:5-8, 5:60-6:7, 11:55-12:19, 14:20-15:14.

Grigg therefore discloses or at least renders obvious claim 4. Cockburn ¶¶155-160.

6. Claim 5

a. "The method of claim 3, wherein the biometric scan includes a thumbprint."

Grigg discloses the biometric scan includes a thumbprint. Cockburn ¶¶161-167.

As discussed for claim 3, *Grigg* discloses that its security features to authenticate a user may include a "biometric scan." *Grigg*, 6:45-61, 11:11-23. *Grigg*'s biometric scan may include a "fingerprint scan." *Grigg*, 2:54-59, 11:24-32, 11:43-12:19, 14:52-15:4, 18:30-40, 20:66-21:2, 21:58-62.

Grigg's mobile device "compare[s] … the fingerprint scan with the previously stored image of the user's fingerprint" to authenticate a user. *Grigg*, 11:55-67, 11:24-32 (receiving an input via "a touch screen … associated with the user's mobile device"), 11:43-54 (storing security features that include "a scanned fingerprint for use with fingerprint scanning software"), 15:1-4 (optionally requiring "a fingerprint scan must have 90% similarity with a saved fingerprint before authenticating the user's identity").

A POSITA would have understood that *Grigg*'s "fingerprint" discloses the claimed "thumbprint" because a thumb is a "finger" and a thumb has a fingerprint. Cockburn ¶¶161-164. It was known to analyze a user's fingerprint from their thumb as it is typically facing a mobile device's touchscreen or fingerprint reader while holding the mobile device. Cockburn ¶164 (citing Ex-1027 ¶14). This is also consistent with the ’347 patent, which discloses that “[t]he third security level is set by entering a user-selected ***fingerprint*** 324 that identifies the user.” Ex-1001, 10:47-48.

To the extent *Grigg*’s fingerprint does not disclose a “thumbprint,” *Grigg* renders this obvious. Cockburn ¶165. A POSITA would have understood that thumbs include a fingerprint just like every other digit and thus a fingerprint scan includes a scan of a finger or thumb. *Id.* (citing Ex-1022, 1). A POSITA would have modified *Grigg* to capture a “thumbprint,” to the extent *Grigg* does not disclose this expressly, to capture any digit of a user. *Id.* This includes the thumb, which most smartphones (like those in *Grigg*) are designed to capture for fingerprint scanning. *Id.* (citing Ex-1023, 53-54 (Fig. 11); Ex-1024, 1). This modification would have been nothing more than combining known elements in the prior art with understood and predictable results. *Id.*

As discussed, *Grigg*—as disclosed or modified—would have included a first single security level scan that includes a request for a password and one or more additional security level scans that include biometric information such as a fingerprint sample, which may include analyzing the fingerprint of a user’s thumb. Cockburn ¶166; *see* Elements [1b], [1d]. The user would provide a fingerprint by their thumb via a touchscreen or fingerprint reader in *Grigg*’s mobile device for comparison to the stored security features (e.g., a stored fingerprint image) for authenticating the user. Cockburn ¶166; *see, e.g.*, *Grigg*, 2:50-64, 3:28-41, 5:5-8, 5:60-6:7, 11:55-12:19, 14:20-15:14.

Grigg therefore discloses or at least renders obvious claim 5. Cockburn ¶¶161-167.

7. Independent Claim 6

a. [6pre]: "A system for securely accessing a local application on a mobile device, comprising the steps of:"

Grigg discloses a system for securely accessing a local application on a mobile device. Cockburn ¶¶168-171.

As discussed for Element [1pre], *Grigg* discloses a method of securely accessing a local application on a mobile device. *See* Element [1pre].

Grigg also discloses that its mobile device is a "financial transaction security system" or "mobile transaction device security system" to describe its operation. *Grigg*, Abstract ("[t]he financial transaction security system receives a security protocol from a user"), 2:4-20 ("mobile transaction device security system" and "financial transaction security system"), 2:50-64 ("financial transaction security system"), 2:65-3:14 (same), 3:54-67, 4:48-52 ("mobile transaction device security system 100"), 6:14-17 ("financial transaction security system"), 10:58-62 (same), 12:35-15:42 (same), 15:44-18:50 (same). System 400, which in one embodiment is the financial transaction security system, may be implemented "as a mobile phone, PDA, keychain fobs, watch, computer, server, electronic device, etc.," including "a memory device 402, a communication device 404, and a processing device 406." *Grigg*, 12:35-49, Fig. 4.

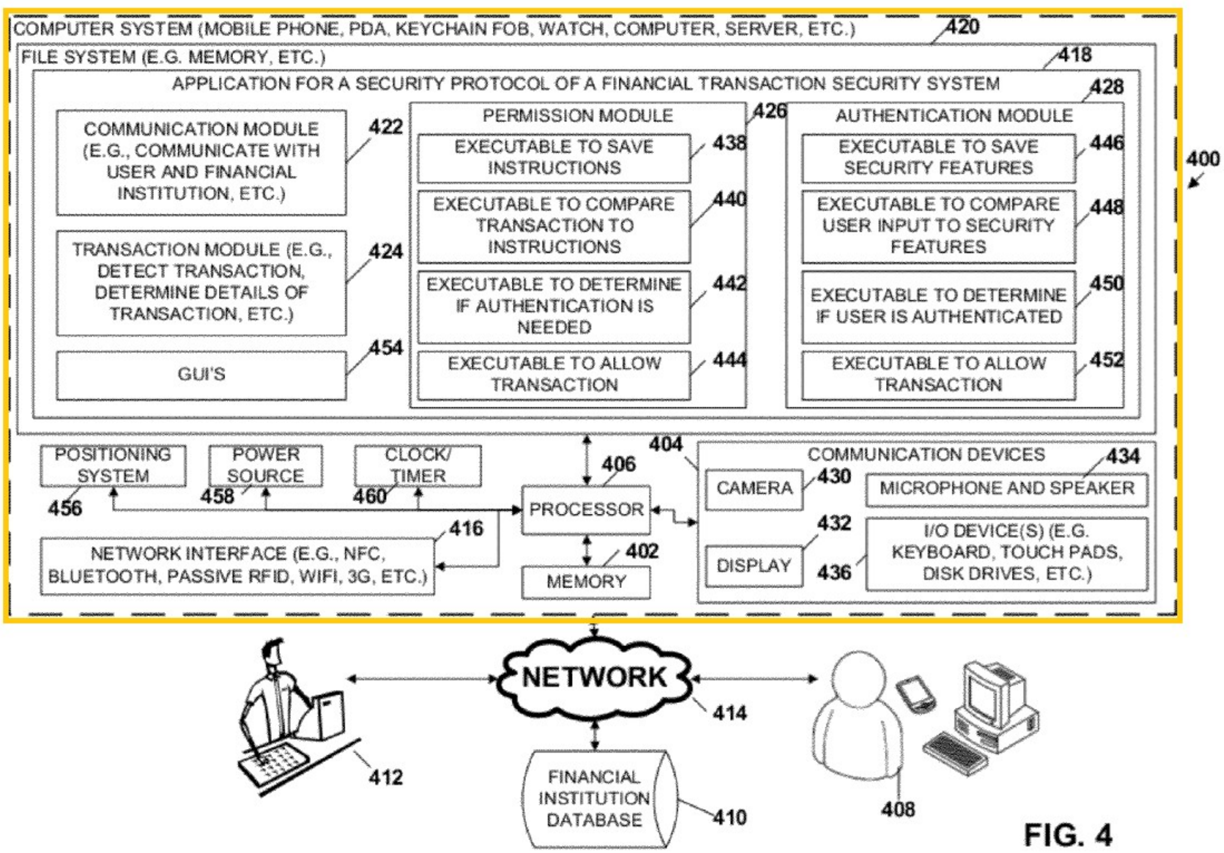


FIG. 4

Grigg, Fig. 4 (annotating system 400, e.g., "COMPUTER SYSTEM (MOBILE PHONE, PDA, KEYCHAIN FOB, WATCH, COMPUTER, SERVER, ETC."); Cockburn ¶170.

Grigg's financial transaction security system, implemented for example as a mobile phone, smartphone, PDA or the like, is the "system," as claimed. Cockburn ¶¶168-171.

b. [6a]: "a hardware processor on a mobile device; and"

Grigg discloses a hardware processor on the mobile device. Cockburn ¶¶172-175.

Grigg's mobile device includes a hardware processor. Cockburn ¶¶173-174. For example, financial transaction security system 400 may be "a mobile phone, PDA, keychain fobs, watch, computer, server, electronic device, etc.," including "a memory device 402, a communication device 404, and a ***processing device 406***." *Grigg*, 12:35-49, 12:57-13:10, 18:51-67, Fig. 4 (illustrating "processor 406").

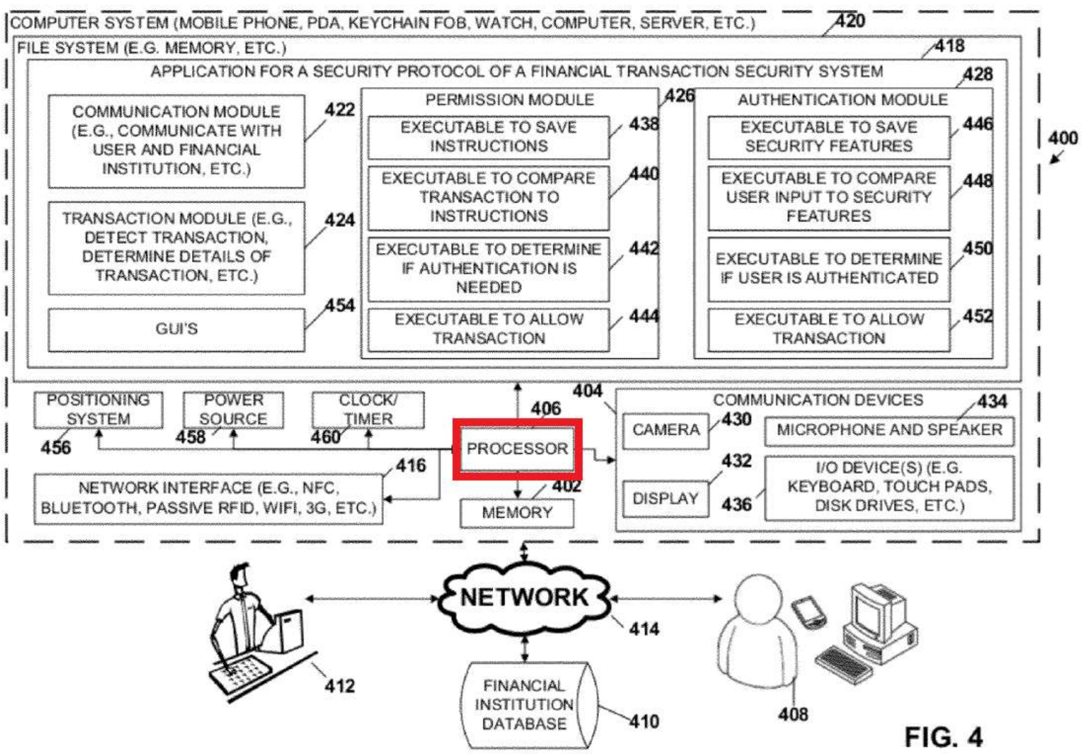


FIG. 4

Grigg, Fig. 4 (annotating **processor 406**); Cockburn ¶174.

Grigg thus discloses a hardware processor on the mobile device. Cockburn ¶¶172-175.

c. [6b]: "a local application on the mobile device and configured to be executed by the hardware processor;"

As discussed for Element [1pre] and [1a], *Grigg* discloses a "local application" that is executed by the processor, including its mobile application or "security protocol application 418." *See* Elements [1pre], [1a]; *Grigg*, 4:48-64, 3:27-41, 6:14-28, 13:11-65, 15:15-23, Fig. 4.

Grigg thus discloses a hardware processor and a local application on the mobile device that is configured to be executed by the hardware processor. Cockburn ¶¶176-177.

d. [6c]: "the local application including a first interface enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application,"

For the reasons explained in Element [1b], *Grigg* discloses and/or renders obvious "the local application … enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application." *See* Element [1b]; Cockburn ¶¶178-181.

Grigg also discloses "a first interface" to do so. For example, *Grigg* discloses that a user "enters the security protocol into ***an interface*** on a mobile device application." *Grigg*, 4:48-63. *Grigg* also discloses that the security protocol application 418 "includes Graphical User Interfaces (GUI's) 454" that assist in communication between the user 408 and the system." *Grigg*, 15:15-23. *Grigg* discloses different GUIs for different functions: "***[m]ultiple GUI's*** 454 can be available for the communication module 422, the transaction module 424, the permission module 426, and the authentication module 428." *Grigg*, 15:15-23. Thus, *Grigg* discloses an interface to set permissions via permission module 426 and an interface to authenticate a user via authentication module 428. *Grigg*, 15:15-23; Cockburn ¶179. As discussed for Elements [1b] and [1d], in the modified *Grigg* system, the user would set the desired security level configuration setting via, for example, *Grigg*'s interface 900 and authenticate the user via *Grigg*'s authentication module. *See* Elements [1b], [1d]; Cockburn ¶180. *Grigg* provides exemplary depictions of this interface in Figure 9. *Grigg*, 17:49-18:50, Fig. 9.

Grigg therefore discloses and/or renders obvious Element [6c]. Cockburn ¶¶178-181.

e. [6d]: "the local application including a second interface requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels."

For the reasons explained in Element [1d], *Grigg* discloses or at least renders obvious "the local application … requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels." *See* Element [1d]; Cockburn ¶¶182-184.

For the reasons explained in Element [6c], *Grigg* discloses an interface or GUI for authenticating a user and thus discloses the claimed "second interface." *See* Element [6b]; *Grigg*, 15:15-23; Cockburn ¶183. *Grigg* also discloses that system 100 "can provide ***a prompt on a display screen*** of a mobile device requesting entry of a user name and password." *Grigg*, 5:49-59. *Grigg*'s "system may receive the input [for authentication] from the keyboard, ***a touch screen***, a microphone, and/or a camera associated with the user's mobile device. *Grigg*, 11:24-32. *Grigg*'s GUIs for authenticating a user during a transaction, including "prompt[ing] on a display screen" for input, discloses the "second interface," as claimed. Cockburn ¶183.

Grigg therefore discloses or at least renders obvious Element [6d]. Cockburn ¶¶182-184.

8. Claim 7

a. "The system of claim 6, wherein the single security level scan includes a request for a password."

Grigg and modified *Grigg* discloses the additional limitation in claim 7 for the same reasons discussed for claim 2. Cockburn ¶185.

9. Claim 8

a. "The system of claim 6, wherein the plurality of security level scans includes a biometric scan."

Grigg discloses or at least renders obvious the additional limitation in claim 8 for the same reasons discussed for claim 3. Cockburn ¶186.

10. Claim 9

a. "The system of claim 8, wherein the biometric scan includes a voiceprint."

Grigg discloses or at least renders obvious the additional limitation in claim 9 for the same reasons discussed for claim 4. Cockburn ¶187.

11. Claim 10

a. "The system of claim 8, wherein the biometric scan includes a thumbprint."

Grigg discloses or at least renders obvious the additional limitation in claim 10 for the same reasons discussed for claim 5. Cockburn ¶188.

B. Ground 2: Claims 1-10 Are Rendered Obvious by *Grigg* in View of *Carter*

1. Overview of *Carter*

Like *Grigg*, *Carter* discloses methods for authenticating a user of a mobile device while conducting a transaction. *Carter*, Abstract, ¶¶[0005]-[0008]; Cockburn ¶¶61-62. In embodiments, *Carter* discloses authenticating a user by fingerprint validation, voice validation, facial recognition validation, iris scan validation, PIN validation, and GPS location validation. *Carter* ¶¶[0007], [0031]-[0040]. *Carter*'s mobile device is "configured for multi-factor authentication of transactions" and includes "levels" of authentication based on transaction value, where "each increasing level of authentication may cumulatively require authentication by all of the methods of each lower level in the hierarchy." *Carter* ¶¶[0031]-[0032].

2. Motivation to Combine *Grigg* with *Carter*

A POSITA would have been motivated to improve *Grigg* in view of *Carter*—to the extent *Grigg* alone does not already disclose or render obvious this improvement—to provide a mobile device that authenticates a user using one or more levels as specified by a user. Cockburn ¶¶189-196.

A POSITA first would have understood *Grigg* and *Carter* were compatible. Cockburn ¶191. Both disclose methods of using a mobile device in a transaction, including payments at a point-of-sale location, *Grigg*, 2:4-20, 2:50-64, 3:28-40; *Carter* ¶¶[0008], [0047], [0068], and disclose similar types of mobile devices. *Grigg*, 3:15-22, 12:35-40; *Carter* ¶[0020]. Both also focus on protecting a user's sensitive information. *Grigg*, 1:57-60, 2:4-7; *Carter* ¶¶[0031]-[0032], [0104]. *Grigg* and *Carter* further contemplate security "levels" for authenticating a user. *Grigg*, 7:55-60, 8:35-41, 14:63-15:4; *Carter* ¶¶[0006], [0031]-[0040]. Given the overlap of *Grigg* and *Carter*, in addition to the similar problems they address, a POSITA would have understood they were compatible. Cockburn ¶191.

Carter is also analogous art to the '347 patent because both are from the same field of endeavor: application security to protect a user's sensitive information. Cockburn ¶192. Like the '347 patent, *Carter* improves the security of applications by providing levels of authentication during a transaction. *Carter*, ¶¶[0006], [0031]-[0040]. The '347 patent is similarly directed to securing a mobile application by requiring one or more authentication levels. Ex-1001, Abstract, 10:32-11:41. *Carter* is therefore analogous art to the '347 patent. Cockburn ¶192.

To the extent *Grigg* alone does not disclose and/or render obvious allowing a user to choose between single and multiple authentication levels (*Grigg* does), a POSITA would have looked to *Carter* to incorporate this feature. Cockburn ¶193. Doing so would have enabled a user to choose single level or multiple levels of user authentication based on, for example, a user preference for greater security or the details of the transaction. *Id.* Indeed, *Carter* expressly discloses different authentication "levels" to secure a transaction, just like *Grigg*, and expressly contemplates "cumulative" levels. *Carter* ¶¶[0031]-[0032]; *Grigg*, 6:37-61.

A POSITA would have been motivated to combine *Grigg* with *Carter* for the reasons *Carter* explains, including "reliably authenticating transactors electronically" to avoid "the danger of fraud." *Carter* ¶[0003]; Cockburn ¶194. *Carter* discloses requiring "greater authentication … for higher value (and higher risk) purchases," which "greatly decrease[s]" the risk of fraud. *Carter* ¶[0032]. This includes "requir[ing] different types of authentication." *Id.* A POSITA thus would have been motivated to modify *Grigg* in view of *Carter* to use one or more levels of authentication and "different types of authentication" to improve security, prevent fraud, and to more accurately authenticate a user in a transaction. Cockburn ¶194. This includes, for example, incorporating a user preference for one or more authentication levels, or incorporating *Carter*'s authentication levels based on transaction amounts. *See Carter* ¶¶[0032]-[0039].

A POSITA would have had a reasonable expectation of success in the combination because *Grigg* emphasizes user-customization and *Carter* discloses the ability of a user to select between different levels of authentication. *See, e.g.*, *Grigg*, 5:29-31, 8:38-41, 10:40-43; *Carter* ¶¶[0032]-[0040]; Cockburn ¶195. POSITAs also understood that multi-factor authentication was known and understood in the art, and *Carter* expressly discloses its use in the same context as *Grigg*: in a financial transaction at a point-of-sale location. Cockburn ¶195.

A POSITA would have known that requiring more than one type of authentication as contemplated by *Grigg* and *Carter*, including a password and biometric information, would have improved the security of a financial transaction in the combined system. *Id.* For example, it is more difficult to fraudulently conduct a transaction when multiple factors are required. *Id.* Based on user preference for any transaction, or for certain high value/high risk transactions, a user would be able to set the system to require something a user knows (e.g., a password) and something the user is (e.g., biometric information such as a fingerprint, facial scan, voice sample, etc.). *Id.* In other situations, the user would be able to set the system to require only one factor. *Id.*

Combining *Grigg* with *Carter*'s cumulative levels of authentication would have been nothing more than combining known elements in the prior art with expected results. Cockburn ¶196. The resulting combination would have been a system that enables a user to set a preference for one or more authentication levels before allowing a transaction to proceed. *Id.* Alternatively, the combination would have enabled a user to set a transaction threshold under which only one authentication technique is required (e.g., a password) and at or above which an additional (and different) authentication technique is required (e.g., biometric information). *Id.* Only after a user is authenticated by the one or more authentication methods would a transaction be allowed. *Id.* Modifying *Grigg* in this manner would have been well within the capabilities of a POSITA because both *Grigg* and *Carter* contemplate levels of security for mobile devices transactions, and POSITAs understood how to implement user interfaces to enable such functionality. *Id.*

3. Independent Claim 1

a. [1pre]: "A method of securely accessing a local application on a mobile device, comprising the steps of:"

Grigg discloses Element [1pre] for the same reasons discussed in Grounds 1A and 1B, Element [1pre]. Cockburn ¶197.

b. [1a]: "launching a local application on a mobile device;"

Grigg discloses Element [1a] for the same reasons discussed in Grounds 1A and 1B , Element [1a]. Cockburn ¶198.

c. [1b]: "enabling a user to set a desired security level configuration setting in the local application for the mobile device, the desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application"

Grigg in view of *Carter* renders this feature obvious. Cockburn ¶¶199-208.

As discussed in Grounds 1A and 1B, Element [1b], *Grigg* discloses enabling a user to set a desired security level configuration setting in the local application for the mobile device before allowing access to at least a feature in the local application. Cockburn ¶200.

Carter discloses a desired security level configuration setting establishing whether a single security level or a plurality of security levels is required before allowing access to at least a feature in the local application. Cockburn ¶201.

For example, *Carter* discloses "receiv[ing] information related to the person that can be used for authentication purposes," including biometric information, and "authenticat[ing] the person by verifying the information received." *Carter* ¶[0005]. A hierarchy of "authentication ***levels***, where each authentication level requires a different authentication method" can be used to authenticate a user, where "***each level*** of the hierarchy may require the ***cumulative authentication methods*** of one or more of the lower levels in the hierarchy." *Carter* ¶[0006]. *Carter* thus discloses a desired security level configuration setting in its authentication levels. Cockburn ¶202.

Carter also discloses a user setting a desired security level configuration setting by assigning particular authentication levels based on a "person's preferences" or "the value of the transaction." *Carter* ¶¶[0032], [0040]; Cockburn ¶203. This may include "transaction controls" specifying the level of authentication required for a transaction. *Carter* ¶¶[0068]-[0069], ¶[0040], ¶[0032]; *see also Carter* ¶[0031]; Cockburn ¶203.

Carter's device 101 "is configured for multi-factor authentication of transactions" and *Carter* discloses various authentication methods for different levels. *Carter* ¶¶[0031]-[0032]. For example, a first level may require fingerprint authentication, a second level may require a personal identification number (PIN), a third level may require voice biometric identification, a fourth level may require facial recognition, and a fifth level may require GPS location authentication. *Carter* ¶¶[0033]-[0039]. The number of levels, the type of authentication for each level, and their order "may be variable and context-specific." *Carter* ¶[0040]; *see also Carter* ¶[0032], ¶[0036].

For *Carter*'s different levels, "each increasing level of authentication may cumulatively require authentication by all of the methods of each lower level in the hierarchy." *Carter* ¶[0032]; *see also Carter* at claim 14, ¶[0006]. *Carter* discloses, like *Grigg*, authentication may include "fingerprint validation, voice validation, facial recognition validation, iris scan validation, PIN validation, and GPS location validation." *Carter* ¶[0007].

Carter discloses that its mobile device may include I/O 109, which includes "at least audio/video output, a keypad and/or touch screen, a microphone, a camera, a GPS transceiver, and a fingerprint reader (which may be included in a touch screen)." *Carter* ¶[0031]. I/O 109 "may include a biometric sensor, which can collect one or more types of biometric data." *Id.*

Carter's user-configurable authentication levels disclose a desired security level configuration setting that establishes whether the local application requires a single security level or a plurality of security levels before allowing access to at least a feature in the local application. Cockburn ¶¶204-207. Like *Grigg*, the "feature" of *Carter*'s local application is the ability to complete a transaction with a mobile device at a point-of-sale location. *Carter* ¶¶[0003]-[0006], [0008], [0031]-[0040]; Cockburn ¶207. Each of *Carter*'s security levels corresponds to a different security level scan (i.e., authentication method(s)). *See Carter* ¶[0069], claim 9. *Carter* discloses setting the security level and thus setting "the desired security level configuration setting" by allowing the user to control the authentication levels based on user preferences and/or transaction details. *Carter* ¶[0032]; *see also Carter* ¶¶[0028], [0040].

In the combined *Grigg*-*Carter* device, a POSITA would have set a desired authentication level based on user preference, which would have required one or more of *Carter*'s authentication methods before enabling the device to perform a transaction. Cockburn ¶208. Alternatively, a user in *Grigg*-*Carter* would set the desired authentication level based on a transaction dollar threshold, above which more than one authentication level is required. *Id.*; *Carter* ¶¶[0040], [0069]. For example, below $100 a user only needs to input a password. Cockburn ¶208. For transactions above $100, the user needs to authenticate herself using multiple, cumulative security levels, including a password and biometric information. *Id.* A POSITA would have implemented *Carter*'s optional authentication levels and hierarchy in *Grigg*'s user interface, for example in setting permissions via interface 800. *Id.*

d. [1c]: "launching the local application after the setting of the desired security level configuration setting; and"

Grigg discloses Element [1c] for the same reasons discussed in Grounds 1A and 1B, Element [1c]. Cockburn ¶209.

e. [1d]: "requiring, before allowing access to the at least one feature of the local application, the user to perform an authentication process based on the desired security level configuration setting, the authentication process including only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels."

Grigg discloses requiring, before allowing access to the feature of the local application, the user to perform an authentication process based on the desired security level configuration setting for the same reasons discussed in Grounds 1A and 1B, Element [1d]. Cockburn ¶¶210-215.

To the extent *Grigg* alone does not disclose or render it obvious, *Grigg* in view of *Carter* also renders obvious doing so where the authentication process includes only a single security level scan when the desired security level configuration setting is set to a single security level, the authentication process including a plurality of security level scans when the desired security level configuration setting is set to a plurality of security levels. Cockburn ¶211.

For example, *Carter* discloses that "the person (customer) initiates the transaction" and "a determination is made whether the aspects of the transaction match pre-set purchasing preferences, which involves personal information supplied at 203A and information about the transaction supplied at 203B." *Carter* ¶[0068]. "If the transaction matches the preferences, the transaction must then be authenticated before proceeding," where the necessary authentication level is determined "based on the transaction criteria." *Carter* ¶[0069]. *Carter* explains that "the necessary level and type of authentication for various transactions may be controlled, at least in part, by the person's preferences." *Carter* ¶[0032]. This includes, for example, "the person may hav[ing] at least some control over the specific values where the authentication level changes." *Id.*; *see also Carter* ¶¶[0068]-[0069], claim 15; Cockburn ¶212. In some embodiments, user preferences or different transaction amounts can trigger different levels of authentication. *Carter* ¶¶[0033]-[0040].

In the combined *Grigg-Carter* system, a user would have set the desired level of authentication based on a user preference or alternatively based on a dollar amount for a transaction. *See* Element [1b]. The mobile device would then determine when a user is engaged in a transaction and implement the set level of authentication before allowing the transaction to proceed. *See* Element [1c] (Grounds 1A, 1B); *Grigg*, 5:12-31, 9:32-42, 13:36-44; *Carter* ¶[0068]; Cockburn ¶213.

It would have been obvious to require one or more of *Carter*'s authentication levels based on user preferences or based on a transaction threshold in the combined system. *Carter* ¶[0032]; Cockburn ¶214. Based on the user preference, one authentication method or multiple cumulative methods are required before allowing a transaction to proceed. Cockburn ¶214. Using transaction data, it would have been obvious for a user to set a threshold of, for example, $100, under which only a password is required to authenticate a user. *Id.*; *Grigg*, 5:5-8, 5:60-6:8, 10:62-12:19, 14:20-15:14. At or over this threshold, a password and biometric information is necessary to authenticate the user, as *Carter* discloses in its "cumulative" levels of authentication. Cockburn ¶214; *Carter* ¶¶[0006], [0032], claim 14. It would have been obvious to combine *Grigg* and *Carter* in this manner as described in Section VII.B.2 ("Motivation to Combine *Grigg* with of *Carter*").

Grigg in view of *Carter* therefore renders Element [1d] obvious. Cockburn ¶215.

4. Claim 2

In *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 2 for the same reasons discussed for claim 2, Grounds 1A and 1B. Cockburn ¶216.

5. Claim 3

In *Grigg-Carter*, *Grigg* discloses the additional limitation of a "biometric scan" in claim 3 for the same reasons discussed for claim 3, Grounds 1A and 1B. Cockburn ¶217. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the "plurality of security level scans." *Carter* ¶¶[0031], [0033]-[0039]; Cockburn ¶217; *see also* Element [1b], Ground 2.

6. Claim 4

In *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 4 for the same reasons discussed for claim 4, Grounds 1A and 1B. Cockburn ¶218. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the "plurality of security level scans." *Carter* ¶¶[0031], [0033], [0035]-[0038]; Cockburn ¶218.

7. Claim 5

In *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 5 for the same reasons discussed for claim 5, Grounds 1A and 1B. Cockburn ¶219. *Carter* also discloses this feature in addition to rendering obvious a biometric scan being one of the "plurality of security level scans." *Carter* ¶¶[0031], [0033]-[0036], [0038]; Cockburn ¶219.

8. Independent Claim 6

a. [6pre]: "A system … :"

In *Grigg-Carter*, *Grigg* discloses the additional limitation in Element [6pre] for the same reasons discussed for Element [6pre], Grounds 1A and 1B. Cockburn ¶¶220.

b. [6a]: "a hardware processor on a mobile device; and"

In *Grigg-Carter*, *Grigg* discloses the additional limitation in Element [6a] for the same reasons discussed for Element [6a], Grounds 1A and 1B. Cockburn ¶221.

a. [6b]: "a local application … "

In *Grigg-Carter*, *Grigg* discloses the additional limitation in Element [6b] for the same reasons discussed for Element [6b], Grounds 1A and 1B. Cockburn ¶223.

b. [6c]: "the local application including a first interface enabling … ,"

In *Grigg-Carter*, *Grigg* discloses the "first interface" in Element [6c] for the same reasons discussed for Element [6c], Grounds 1A and 1B. Cockburn ¶223.

Grigg in view of *Carter* renders obvious the additional limitations in Element [6c] for the same reasons discussed for Element [1b], Ground 2. Cockburn ¶224.

c. [6d]: "… perform an authentication process …"

In *Grigg-Carter*, *Grigg* discloses the "second interface" in Element [6d] for the same reasons discussed for Element [6d], Grounds 1A and 1B. Cockburn ¶225.

Grigg in view of *Carter* renders obvious the additional limitations in Element [6d] for the same reasons discussed for Element [1d], Ground 2. Cockburn ¶226.

9. Claim 7

In *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 7 for the same reasons discussed for claim 2, Grounds 1A and 1B. Cockburn ¶227.

10. Claim 8

In *Grigg-Carter*, *Grigg* discloses or at least renders obvious the additional limitation of a "biometric scan" in claim 8 for the same reasons discussed for claim 3, Grounds 1A and 1B. Cockburn ¶228. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the "plurality of security level scans." *Carter* ¶¶[0031], [0033]-[0039]; Cockburn ¶228; *see also* Element [1b], Ground 2.

11. Claim 9

In *Grigg-Carter*, *Grigg* discloses or at least renders obvious the additional limitation in claim 9 for the same reasons discussed for claim 4, Grounds 1A and

1B. Cockburn ¶229. *Carter* also discloses this feature. *Carter* ¶¶[0031], [0033], [0035]-[0038]; Cockburn ¶229.

12. Claim 10

In *Grigg-Carter*, *Grigg* discloses or at least renders obvious the additional limitation in claim 10 for the same reasons discussed for claim 5, Grounds 1A and 1B. Cockburn ¶230. *Carter* also discloses this feature. *Carter* ¶¶[0031], [0033]-[0036], [0038]; Cockburn ¶230.

C. Grounds 3A and 3B: Claims 1, 2, 6, and 7 Are Anticipated and/or Rendered Obvious by *Google*

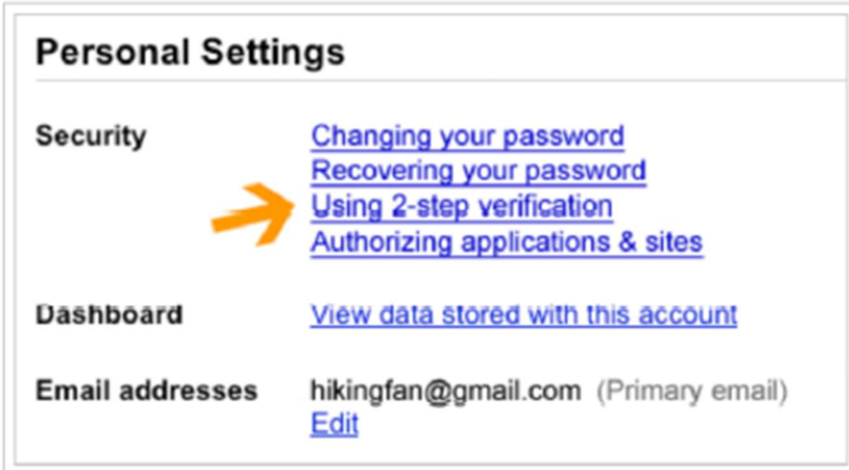
1. Overview of *Google*

According to *Google*, "[t]here are plenty of examples (like the classic 'Mugged in London' scam) that demonstrate why it's important to take steps to help secure your activities online." *Google*, 1. As *Google* explains, "if you reuse the same password on multiple sites and one of those sites gets hacked, or your password is conned out of you directly through a phishing scam, it can be used to access some of your most closely-held information." *Id.* This information may include "[y]our Gmail account, your photos, your private documents." *Id.*; Cockburn ¶¶63-64.

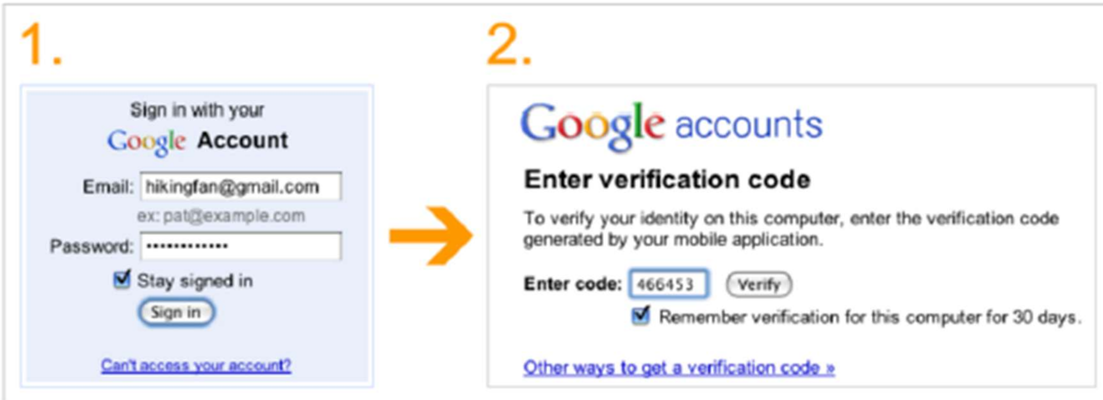
To further strengthen the security offered by a single password, *Google* discloses "an advanced opt-in security feature called 2-*step verification* that makes your Google Account significantly more secure by helping to verify … the real owner of your account." *Google*, 1 (emphasis in original). According to *Google*, "2-step verification requires two independent factors for authentication … : your password, plus a code obtained using your phone." *Id.*; Cockburn ¶65.

Authentication for a Google Account is a prerequisite to using certain *Google* applications, including Gmail. Cockburn ¶66 (citing Ex. 1014, 30:61-65 (discussing the use of "a Google account for accessing one or more web based services such as Gmail, Google calendars, Google reader, etc.")). Once authenticated, Gmail can be accessed on a mobile device in at least two different ways. Cockburn ¶67. First, a user may launch an internet browser on a mobile device and access Gmail via Gmail's mobile website. Cockburn ¶68 (citing Ex-1008, [0022] (describing Gmail as a "web-based email service"); Ex-1009, 16:48-49 (describing Gmail as "the most 'green' mobile site we found")); Ex-1013, 20:4-12. Second, a user may download a standalone Gmail application on a mobile device. Cockburn ¶69 (citing Ex-1010, 20:14-19 ("One example of such a client based email application is a mobile version of GMail™ developed by Google Inc. In some embodiments, a mobile version of a client based application is different from a version that is browser based."); Ex-1013, 20:4-12).

Google explains that security for accessing a *Google* Account can be adjusted using the following interface:



Google, 1; Cockburn ¶70. From this "Account Overview," a user can elect to opt in to 2-step verification or continue with simply a username/password. *Google*, 1; Cockburn ¶¶71-72. In the event a user selects 2-step verification, a user must enroll using "[a] user-friendly set-up wizard," which includes "setting up a backup phone and creating backup codes in case you lose access to your primary phone." *Google*, 1. As *Google* explains, "[o]nce you enable 2-step verification, you'll see an extra page that prompts you for a code when you sign in to your account. After entering your password, Google will call you with the code, send you an SMS message or give you the choice to generate the code for yourself using a mobile application." *Id.* The interfaces for the username/password and verification code are shown below:



Id.

Google is analogous art to the ’347 patent. Cockburn ¶73. Both *Google* and the ’347 patent are from the same field of endeavor: application security to protect a user’s sensitive information. *Id.* Like the ’347 patent, *Google* seeks to improve the security associated with applications containing sensitive information with a multi-layered approach to authentication. *Google*, 1; Ex-1001, Abstract, 10:32-53.

2. Independent Claim 1

a. [1pre]: “A method … :”

To the extent the preamble is limiting, *Google* discloses it. Cockburn ¶¶231-233. *Google* discloses a method of securely accessing a Google Account, including Google’s mailbox provider, Gmail. *Google*, 1.

A POSITA would have understood that Gmail was accessible from a web browser (“a local application”) on a mobile device. Cockburn ¶232 (citing Ex-1008, [0022] (describing Gmail as a “web-based email service”); Ex-1009, 16:48-49 (describing Gmail as "the most 'green' mobile site we found")). A POSITA would have also understood that Gmail is also accessible via a mobile application ("a local application") on a mobile device (referred to below as "Gmail mobile application"). *Id.* (citing Ex-1010, 20:14-19; Ex-1013, 20:4-12).

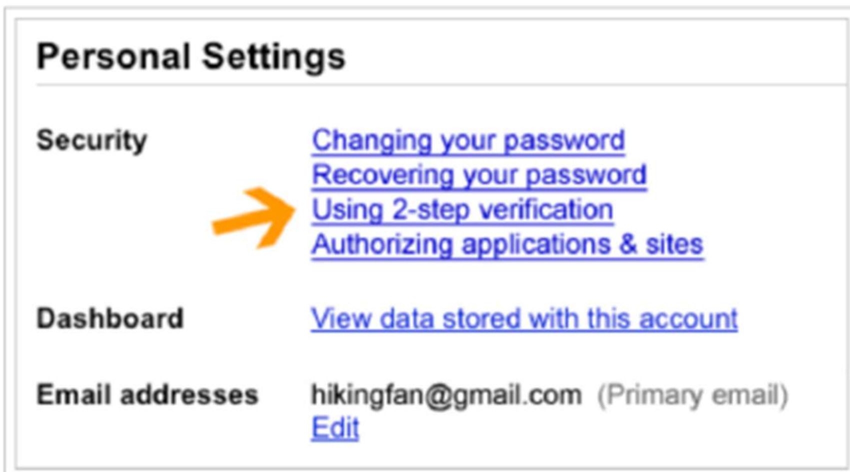
To further strengthen the security offered by a single password, *Google* discloses "an advanced opt-in security feature called 2-*step verification* that makes your Google Account [(including, e.g., Gmail)] significantly more secure by helping to verify … the real owner of your account." *Google*, 1 (emphasis in original). A POSITA would have understood that *Google*'s "advanced opt-in security feature" enhanced the security of Google's Gmail, whether accessed via a browser or mobile application on a mobile device. Cockburn ¶233. Thus, to the extent the preamble is limiting, it is disclosed by *Google*. *Id.*

b. [1a]: "launching … ;"

Google discloses [1a]. Cockburn ¶234. As discussed, Gmail is a mailbox provider available through a *Google* Account and accessible from either a mobile phone browser or mobile application. *Google*, 1; Cockburn ¶234. A POSITA would thus understand that Gmail can be accessed by launching a web browser ("a local application") or mobile application ("a local application") on a mobile device. Cockburn ¶234.

c. [1b]: "enabling … "

Google discloses and/or renders obvious [1b]. Cockburn ¶¶235-240. Once a user launches a web browser or mobile application to access Gmail, a user may access an "Account Settings page," which "looks like this:"



Google, 1. According to *Google*, using this interface, a user can decide between the default, password-only, security feature ("a single security level") or elect "an advanced opt-in security feature called 2-*step verification*" ("a plurality of security levels"). *Id.* (emphasis in original). *Google* discloses that "2-step verification requires two independent factors for authentication, much like you might see on your banking website: your password, plus a code obtained using your phone." *Id.*

A POSITA would have understood that an "opt-in" feature requires a user to specifically turn on that feature to enable it. Cockburn ¶¶235-237. As *Google* explains, "it may take up to 15 minutes to enroll" in 2-step verification through the use of "[a] user-friendly set-up wizard." *Google*, 1. The result is that a user may choose to (1) maintain only the default password security requirement (i.e., "a single security level") or (2) "opt" in 2-step verification (i.e., "a plurality of security levels"). Cockburn ¶237.

Thus, using *Google*'s Account Settings interface on a mobile phone's web browser or Gmail mobile application, a user may establish whether the browser or mobile application ("local application") require a single security level or a plurality of security levels before allowing access to Gmail's contents ("a feature in the local application"). Cockburn ¶238. Likewise, using *Google*'s Account Settings interface on in the Gmail mobile application, a user may establish whether the Gmail mobile application ("local application") requires a single security level or a plurality of security levels before allowing access to Gmail's contents ("a feature in the local application"). Cockburn ¶238.

To the extent not disclosed, a POSITA would have been motivated to modify the Gmail mobile application to allow access to *Google*'s Account Settings. Cockburn ¶239. Such a modification would improve a user's experience, by placing all related functionality in a single location (i.e., the mobile application), rather than requiring a user to configure security settings in a mobile browser (or elsewhere) before accessing the mobile application. *Id.* In addition to improving user experience, including this functionality in the mobile application itself would advantageously encourage adoption of 2-step authentication. *Id.* Indeed, *Google* itself teaches that 2-step authentication "makes your Google Account significantly more secure." *Google*, 1. A POSITA would thus be motivated to encourage adoption by adding this functionality to the mobile application. Cockburn ¶239.

A POSITA would have further had a reasonable expectation of success in modifying the Gmail mobile application to allow access to *Google*'s Account Settings. Cockburn ¶240. A POSITA would have understood that mobile applications commonly included functionality that allowed a user to modify security settings, and modifying the Gmail mobile application to include similar functionality would be nothing more than routine or conventional. *Id.*

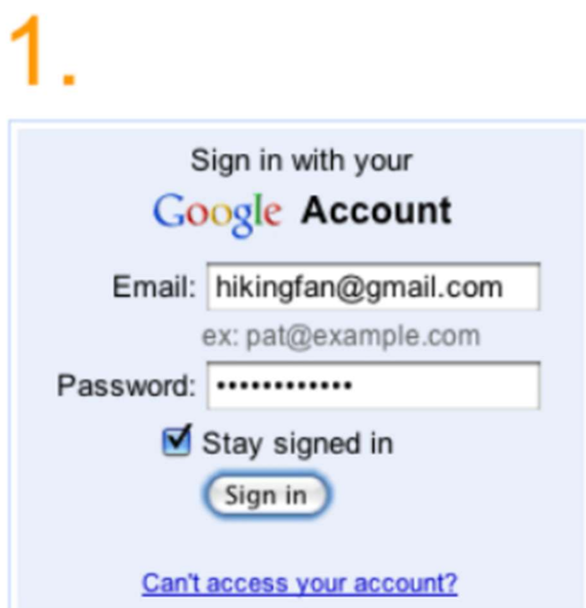
d. [1c]: "launching … "

Google discloses [1c]. Cockburn ¶241. As discussed for [1pre] and [1a], Grounds 3A and 3B, Gmail may be accessed through a web browser ("local application") or mobile application ("local application"). *See* Elements [1pre], [1a]. A POSITA would have understood that, once the security configuration has been established and the browser or mobile application has been closed, a user may again access Gmail by launching the web browser or mobile application on the mobile device. Cockburn ¶241.

e. [1d]: "requiring, … , the user to perform … "

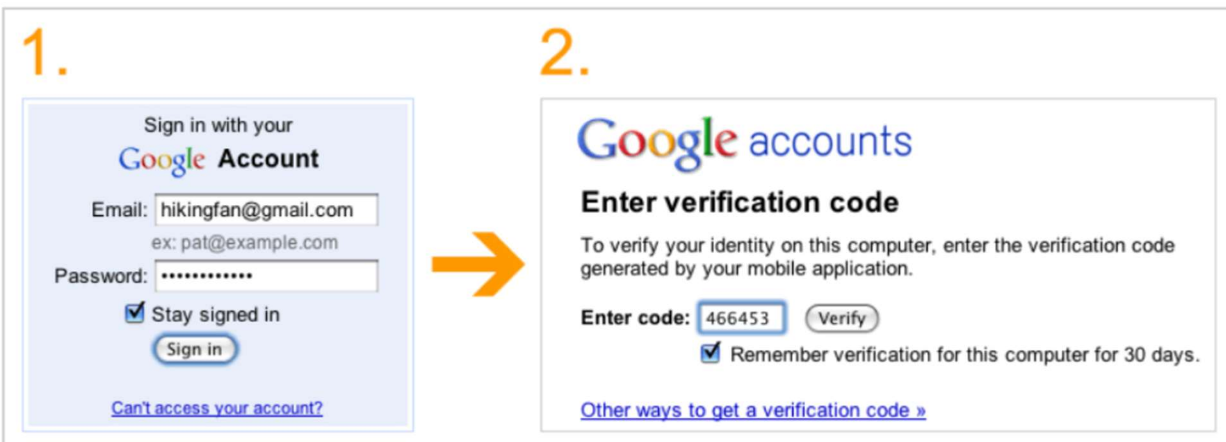
Google discloses [1d]. Cockburn ¶¶242-245. According to *Google*, once a user launches a web browser or mobile application and attempts to access Gmail, the user will be prompted to perform an authentication process before accessing Gmail's contents ("at least one feature of the local application"). *Google*, 1; Cockburn ¶242.

Where a user has declined to opt into 2-factor authentication ("when the desired security level configuration setting is set to a single security level"), the authentication process will only request a password ("the authentication process including only a single security level scan"). *Google*, 1. This is shown below:



Id. (cropped); Cockburn ¶243.

Where a user opts into 2-factor authentication ("when the desired security level configuration setting is set to a plurality of security levels"), the authentication process will request both a password and a code obtained using a phone ("the authentication process including a plurality of security level scans"). *Google*, 1. As *Google* explains and as depicted below, "[o]nce you enable 2-step verification, you'll see an extra page that prompts you for a code when you sign in to your account." *Id.*



Google, 1. "Google will call you with the code, send you an SMS message or give you the choice to generate the code for yourself using a mobile application on your Android, BlackBerry or iPhone device." *Id.* Once this code has been entered, the user can access their Google Account, including Gmail. Cockburn ¶¶244-245.

3. Claim 2

Google discloses the additional limitation in claim 2. Cockburn ¶246. As discussed above, *Google*'s single security level scan includes a request for a password. *Google*, 1.

4. Independent Claim 6

a. [6pre]: "A system … :"

Google discloses or at least renders obvious [6pre] for the same reasons discussed for Element [1pre], Grounds 3A and 3B. Cockburn ¶247.

b. [6a]: "a hardware processor on a mobile device; and"

Google discloses or at least renders obvious [6a]. Cockburn ¶248. As discussed in Element [1pre], Grounds 3A and 3B, a POSITA would have understood that Gmail was accessible from a web browser ("a local application") on a "mobile device," including a "phone" as expressly disclosed in *Google*. *See Google*, 1 (disclosing known examples of mobile devices, including an "Android, BlackBerry or iPhone device"). A POSITA would have known that each of these mobile devices includes a "hardware processor." Cockburn ¶248; Ex-1025, 1 (iPhone 4 "released 2010, June" having a "1.0 GHz Cortex-AB" CPU).

c. [6b]: "a local application … "

Google discloses or at least renders obvious [6b]. Cockburn ¶249. As discussed, *Google* discloses mobile devices, including Android, Blackberry, or an iPhone. *Google*, 1. A POSITA would have understood that each of these devices include a web browser ("a local application") and that such web browsers would necessarily be configured to be executed by the hardware processor. Cockburn ¶249. Similarly, a POSITA would have understood that the Gmail mobile application ("a local application") on the mobile device would necessarily be configured to be executed by the hardware processor. *Id.* This is how mobile phones operate. *Id.*

d. [6c]: "the local application including a first interface enabling … ,"

Google discloses and/or renders obvious [6c] for the same reasons discussed for Element [1b], Grounds 3A and 3B. Cockburn ¶250.

e. [6d]: " … perform an authentication process … "

Google discloses claim [6d] for the same reasons discussed for Element [1d], Grounds 3A and 3B. Cockburn ¶251.

5. Claim 7

Google discloses the additional limitation in claim 7 for the same reasons discussed for claim 2. Cockburn ¶252.

D. Ground 4: Claims 3-5 and 8-10 Are Rendered Obvious by *Google* in View of *Carter*

1. Motivation to Combine *Google* with *Carter*

It would have been obvious to a POSITA to improve *Google*'s 2-factor authentication by including *Carter*'s biometric authentication. Cockburn ¶¶253-258.

As the prior art recognized, access control "has traditionally been handled by passwords or PIN codes. However, these are not personal as they can be given to other persons by the owner, or stolen from the owner." Ex-1011, 1:14-20. As a result, the prior art recognized "a strong trend to base access control on biometrics." Ex-1011, 1:20-25. Unlike a PIN code, biometrics are a "mathematical description of characteristic elements of the owner's body or behaviour that can not be separated from this person, and which describes him uniquely." Ex-1011, 1:20-25. Given that *Google* teaches the use of a pin or code as second form of authentication, a POSITA would have been motivated to instead use a biometric-based access control. Cockburn ¶254.

A POSITA would have understood that biometric-based access control can be based on different elements of a person's body, each with its own benefits. Cockburn ¶255. For example, according to *Carter*, "[e]xamples of various authentication methods include fingerprint validation, voice validation, facial recognition validation, iris scan validation, PIN validation, and GPS location validation." *Carter* ¶[0007].

A POSITA would have understood the benefits associated with using fingerprint scanning, including scanning a thumbprint. Cockburn ¶256. According to *Carter*, "fingerprint authentication can be required for all transactions, due to its ease and simplicity." *Carter* ¶[0034]. A POSITA would have understood that *Carter*'s statement applied equally to a thumbprint. *See* Section VII.A.6.a (Grounds 1A and 1B, claim 5); Cockburn ¶256; *see* Ex-1023, 53-54 (Fig. 11); Ex-1024, 1. As a result, a POSITA would have also been motivated to employ a biometric-based access control using an individual's fingerprint or thumbprint, including *Carter*'s fingerprint validation. Cockburn ¶256. To the extent *Carter*'s fingerprint does not disclose a "thumbprint," *Carter* renders this obvious. Cockburn ¶256; *see infra* claim 5 (Ground 4).

A POSITA would have also understood the benefits associated with using voice validation. Cockburn ¶257. For example, the prior art taught "that there are certain characteristics of an individual's voice which cannot be disguised and which are as effective in identifying an individual as the ridges of his fingerprint." Ex. 1012, 2:4-7. As a result, a POSITA would have also been motivated to employ a biometric-based access control using an individual's voice, including *Carter*'s voice validation. Cockburn ¶257.

A POSITA would have had a reasonable expectation of success in modifying *Google*'s mobile device in view of *Carter*'s methods of biometric authentication. Cockburn ¶258. *Carter* teaches that a "mobile device may contain a biometric sensor to read biometric information." *Carter* ¶[0008]. *Carter* also explains that "a camera, a touch screen, a microphone, etc., can be configured to function as biometric sensors, for collecting data such as facial recognition data, fingerprint data, and voice recognition data, respectively." *Carter* ¶[0031]. Given that *Google*'s Gmail can be accessed from mobile device, as discussed above, a POSITA would have been able to employ that mobile's device's existing functionality for the aforementioned biometric-based access control. Cockburn ¶258. This includes the functionality of the iPhone available as of the critical date. Cockburn ¶258; Ex-1025, 1-2. The modification would have entailed nothing "more than the predictable use of prior art elements according to their established functions." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

2. Claim 3

The *Google*-*Carter* combination renders obvious claim 3. Cockburn ¶259. As discussed in Section VII.D.1, a POSITA would have been motivated to modify the security settings associated with a *Google* Account to include biometric authentication instead of a code or PIN, and would have had a reasonable expectation of success in doing so. Cockburn ¶259. *Carter* teaches the use of a variety of biometric scans, including "fingerprint validation, voice validation, facial recognition validation, [and] iris scan validation." *Carter* ¶[0007].

3. Claim 4

The *Google*-*Carter* combination renders obvious claim 4. Cockburn ¶260. As discussed in Section VII.D.1, a POSITA would have been motivated to modify the security settings associated with a Google Account to include biometric authentication instead of a code or PIN. Cockburn ¶260. As further discussed in Section VII.D.1, a POSITA would have been motivated to use a voiceprint, including *Carter*'s "voice validation," and would have had a reasonable expectation of success in doing so. *Carter* ¶[0007]; Cockburn ¶260.

4. Claim 5

The *Google*-*Carter* combination renders obvious claim 5. Cockburn ¶¶261-262. As discussed in Section VII.D.1, a POSITA would have been motivated to modify the security settings associated with a Google Account to include biometric authentication instead of a code or PIN. As further discussed in Section VII.D.1, a POSITA would have been motivated to use thumbprint, including *Carter*'s "fingerprint validation," and would have had a reasonable expectation of success in doing so. *Carter* ¶[0007]; Cockburn ¶261.

To the extent *Carter*'s fingerprint does not disclose a "thumbprint," *Carter* renders this obvious. Cockburn ¶262. A POSITA would have understood that thumbs include a fingerprint just like every other digit and thus a fingerprint scan includes a scan of a finger or thumb. *See* Ex-1022, 1 ("Fingerprint ridges begin to develop on the skin of the ***thumbs and fingers*** during the third to fourth month of fetal development, being fully developed by the seventh months."); Cockburn ¶262. A POSITA would have modified *Carter* to capture a "thumbprint," to the extent *Carter* does not disclose this expressly, to capture any digits of a user. Cockburn ¶262. This includes the thumb, which most smartphones (like those in *Carter* and *Google*) are designed to capture for fingerprint scanning. *See* Ex-1023, 53-54 (Fig. 11); Ex-1024, 1; Cockburn ¶262. This would have been nothing more than combining known elements in the prior art with understood and predictable results. Cockburn ¶262.

5. Claim 8

The *Google*-*Carter* combination renders obvious the additional limitation in claim 8 for the same reasons discussed for claim 3, Ground 4. Cockburn ¶263.

6. Claim 9

The *Google*-*Carter* combination renders obvious the additional limitation in claim 9 for the same reasons discussed for claim 4, Ground 4. Cockburn ¶264.

7. Claim 10

The *Google*-*Carter* combination renders obvious the additional limitation in claim 10 for the same reasons discussed for claim 5, Ground 4. Cockburn ¶265.

VIII. MANDATORY NOTICES

A. Real Parties-in-Interest

The real parties-in-interest are Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc.

B. Related Matters

PayGeo LLC asserted the ’347 patent in the following litigation: *PayGeo, LLC v. Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc.*, Case No. 2:25-cv-00334-RWS-RSP (E.D. Tex.).

The ’347 patent claims priority to U.S. Patent Application No. 17/189,721, which issued as U.S. Patent No. 11,087,307; U.S. Patent Application No. 17/009,551, which issued as U.S. Patent No. 10,937,018; U.S. Patent Application No. 16/882,006, which issued as U.S. Patent No. 10,796,296; U.S. Patent Application No. 15/786,470, which issued as U.S. Patent No. 10,733,593; U.S. Patent Application No. 14/691,499, now abandoned; U.S. Patent Application No. 13/974,837, now abandoned; and U.S. Patent Application No. 13/185,432, which issued as U.S. Patent No. 8,554,671. U.S. Patent Application No. 18/746,599, now pending, claims priority to the ’347 patent.

C. Lead and Backup Counsel, and Service Information

Lead Counsel	Backup Counsel
Joshua L. Goldberg, Reg. No. 59,369 joshua.goldberg@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-6092 Fax: 202-408-4400	Benjamin A. Saidman, Reg. No. 69,325 benjamin.saidman@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street NW Suite 1400 Atlanta, GA 30363-6209 Phone: 404-653-6510 Fax: 404-653-6444 Nicholas A. Cerulli, Reg. No. 71,900 nicholas.cerulli@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4248 Fax: 202-408-4400 Alexander M. Boyer, Reg. No. 66,599 alexander.boyer@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: 571-203-2759 Fax: 202-408-4400 Christina Ji-Hye Yang, Reg. No. 79,103 christina.yang@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW

Lead Counsel	Backup Counsel
	Washington, DC 20001-4413 Tel: 202-408-4465 Fax 202-408-4400 Christopher B. Anderson, Reg. No. 77,898 christopher.anderson@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street Suite 800 Reston, VA 20190-6023 Phone: 571-203-2765 Fax: 202-408-4400 Connor M. McGregor, Reg. No. 79,634 connor.mcgregor@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue NW Washington, DC 20001-4413 Phone: 202-408-4363 Fax: 202-408-4400

Please address all correspondence to counsel at the addresses above. Petitioner consents to electronic service by email at the above email addresses.

IX. GROUNDS FOR STANDING

Petitioner certifies that the ’347 patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims on the grounds identified herein.

X. CONCLUSION

For the reasons set forth above, Petitioner requests institution of *inter partes* review and cancellation of each challenged claim. The Office may charge any required fees to Deposit Account No. 06-0916.

Dated: October 1, 2025

By: /Joshua L. Goldberg/
Joshua L. Goldberg
Lead Counsel
Reg. No. 59,369

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, Petitioner certifies that the word count of Petitioner's Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, mandatory notices under § 42.8, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 13,963.

Dated: October 1, 2025

By: /Joshua L. Goldberg/
Joshua L. Goldberg
Lead Counsel
Reg. No. 59,369

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105(a), the **Petition for *Inter Partes* Review, the associated powers of attorney, and Exhibits 1001-1029** were served via FedEx Priority Overnight on October 1, 2025, on the correspondence address of record below indicated in the Patent Office's Patent Center for U.S. Patent No. 12,014,347:

Marc A. Sockol
Sheppard, Mullin, Richter & Hampton LLP
650 Town Center Drive, 10th Floor
Costa Mesa, CA 92626

Dated: October 1, 2025

Respectfully submitted,

/Lisa C. Hines/
Lisa C. Hines
Case Manager
Finnegan, Henderson, Farabow,
Garret & Dunner LLP