

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

Petitioners,

v.

PAYGEO, LLC,

Patent Owner.

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

**DECLARATION OF ANDREW COCKBURN, PH.D.
IN SUPPORT OF PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 12,014,347**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Qualifications and Background	2
III.	Materials Considered.....	6
IV.	Legal Standards	8
	A. Level of Ordinary Skill	9
	B. Prior Art.....	10
	C. Anticipation	10
	D. Obviousness.....	10
V.	Technical Background.....	15
VI.	The '347 patent.....	17
	A. Overview of the '347 patent.....	17
	B. Summary of the Prosecution History of the '347 patent.....	20
	C. Claim Construction of Terms in the '347 patent.....	21
VII.	Person of Ordinary Skill in the Art.....	21
VIII.	The Prior Art.....	22
	A. Overview of <i>Grigg</i> (Ex-1005).....	22
	B. Overview of <i>Carter</i> (Ex-1006).....	25
	C. Overview of <i>Google</i> (Ex-1007).....	25
IX.	Opinions on Unpatentability.....	29
	A. Ground 1A and 1B: <i>Grigg</i> Anticipates and/or Renders Obvious Claims 1-10	30
	1. Claim 1	30

2.	Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”	59
3.	Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”	62
4.	Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”	64
5.	Claim 5: “The method of claim 3, wherein the biometric scan includes a thumbprint.”	65
6.	Claim 6.....	68
7.	Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”	75
8.	Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”	75
9.	Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”	75
10.	Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”	75
B.	Ground 2: <i>Grigg</i> in view of <i>Carter</i> Renders Obvious Claims 1-10	75
1.	Motivation to Combine <i>Grigg</i> and <i>Carter</i>	75
2.	Claim 1	80
3.	Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”	87
4.	Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”	88
5.	Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”	88
6.	Claim 5: “The method of claim 3, wherein the biometric scan includes a thumbprint.”	88

7.	Claim 6.....	89
8.	Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”.....	91
9.	Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”.....	91
10.	Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”	91
11.	Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”.....	92
C.	Grounds 3A and 3B: <i>Google</i> Anticipates and/or Renders Obvious Claims 1, 2, 6, and 7	92
1.	Claim 1	92
2.	Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”.....	99
3.	Claim 6.....	99
4.	Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”.....	101
D.	Ground 4: <i>Google</i> in view of <i>Carter</i> Renders Obvious Claims 3-5 and 8-10	102
1.	Motivation to Combine <i>Google</i> and <i>Carter</i>	102
2.	Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”	104
3.	Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”	104
4.	Claim 5: “The method of claim 3, wherein the biometric scan includes a thumbprint.”.....	105
5.	Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”	106

6.	Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”	106
7.	Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”	106
X.	Conclusion	106

I. INTRODUCTION

1. I, Andrew Cockburn, submit this declaration to state my opinions on the matters described below.

2. I have been retained by Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. as an independent expert in this proceeding before the United States Patent and Trademark Office. I am being compensated at the rate of \$600 per hour for time that I spend on this case. No part of my compensation depends on the outcome and I have no other interest in this proceeding.

3. I understand that this proceeding involves U.S. Patent No. 12,014,347 (“the ’347 patent,” Ex-1001), and I have been asked to provide my opinions as to the patentability of the claims of the ’347 patent.

4. I have been asked to consider the validity of certain claims of the ’347 patent based on certain prior art references. I have also been asked to consider the state of the art and prior art available as of July 18, 2011, which is the earliest claimed priority date on the face of the ’347 patent. Based on the prior art discussed in this declaration, it is my opinion that claims 1-10 of the ’347 patent are unpatentable.

II. QUALIFICATIONS AND BACKGROUND

5. Below is a summary of my education, work experience, and other qualifications. My qualifications are stated more fully in my curriculum vitae, which I understand is provided in Ex-1004.

6. In 1988, I was awarded a Bachelor of Science with Honors in Computer Science from the University of York, England.

7. In 1993, I was awarded a Ph.D. from the University of Stirling, Scotland. My thesis was on “Computer Supported Cooperative Work” which relates to forms of group interaction supported on computers.

8. In 1993, I joined the University of Canterbury as a Lecturer in the Department of Computer Science (now the Department of Computer Science and Software Engineering). I was subsequently promoted to a Senior Lecturer, and then an Associate Professor, before my appointment as a Professor in 2010. I currently hold the title of Emeritus Professor.

9. I have over 30 years of experience in the area of Human-Computer Interaction (HCI). The field of HCI is generally concerned with ways of understanding and improving the interaction between humans and computers, with a view to understanding, evaluating, designing, and building new styles of interactions that improve on one or more of the end goals of making computers faster to learn, more intuitive, more efficient to use, and more subjectively satisfying.

10. Throughout my career, I have published the results of many research projects that have involved building new user interfaces or reviewing existing user interfaces for performing a particular task, and evaluating their effectiveness. This includes publications relating to:

- (a) investigating user experiences with web navigation interfaces, for example when using the “back” button on web browsers;
- (b) reviewing and improving various interface schemes for traversing through documents and lists in desktop and mobile computer applications, including zooming, scrolling, and other techniques;
- (c) analyzing new interfaces for text entry on mobile and touch-sensitive devices;
- (d) addressing the problems arising from the small form factor of mobile devices with touch-sensitive displays, including wearable technologies;
- (e) examining the influence of haptic feedback on user performance with mouse and touchscreen input devices;
- (f) evaluating the importance of spatially stable displays in user interfaces; and

- (g) designing, analyzing and evaluating gesture-based input techniques for various user activities, including music data entry, web navigation, text entry, and scrolling.

11. I also have extensive experience in designing and building new user interfaces and reviewing existing user interfaces. This includes a number of projects regarding the design, development, and evaluation of user interfaces that I have undertaken with companies in the computing and HCI industry, such as:

- (a) working with Microsoft Research in 1999 on the development, evaluation, and improvement of user interfaces for web browsing, in particular the mechanisms for revisiting pages (such as through the “back” button or bookmarks);
- (b) working with Digit Wireless in 2002 on the evaluation of user performance for user interfaces for digital text entry on mobile devices;
- (c) working with IBM Almaden Research in 2006 on the design, development, and evaluation of user interfaces for gesture-based text entry on mobile devices;
- (d) working with Logitech on a number of projects from 2006-2010 regarding the design, development, evaluation, and improvement

of user interfaces for next generation mice, including in relation to scrolling and window management tasks;

- (e) working with Hewlett-Packard Research Labs from 2010-2012 on the design and evaluation of gesture-based pointing techniques for remote displays, such as interactive TVs; and
- (f) working with Airbus SAS in 2016 on methods to assist pilots' gesture-based interaction with touchscreens in turbulent environments.

12. Until my retirement this year, I taught a course on HCI for final year undergraduate students and a course on research methods in HCI for postgraduate students at the University of Canterbury.

13. In the past, I have also taught introductory computer programming courses for first year students across disciplines, which included the implementation of graphical user interfaces.

14. Prior to retirement, I managed an active research lab with a number of Ph.D. students, and I continue to supervise Ph.D. students in my position as Emeritus Professor. I have previously supervised fourteen students to successful completion of their Ph.D.s in the field of HCI.

15. The Association for Computing Machinery (ACM) is the world's largest scientific and educational computing society. In 2015, I was elected to the

ACM Special Interest Group on Computer-Human Interaction (CHI) Academy, which honors the principal leaders of the field of HCI.

16. I also annually attend conferences relating to the field of HCI and regularly read journals that cover research in the field of HCI.

17. To keep abreast with industry trends, I regularly read broader journals, magazines, and websites related to computer science and technology, including Communications of the ACM, ACM TechNews, BBC Technology, and New York Times Technology.

18. I have also consulted on technologies related to fingerprint authentication on mobile devices and lock screen security and authentication in mobile devices. A summary of my complete qualifications can be found in my CV.

19. In light of the foregoing, I believe that I am qualified to provide an opinion as to what a person of ordinary skill in the art would have understood, known, or concluded regarding the subject matter of the '347 patent at the time of its alleged invention.

III. MATERIALS CONSIDERED

20. In forming my opinions, I have reviewed the entirety of the '347 patent and its file history and the following documents:

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-1005	U.S. Patent No. 8,195,576 to Grigg et al. (“ <i>Grigg</i> ”)
Ex-1006	U.S. Patent Application Publication No. 2009/0152343 to Carter (“ <i>Carter</i> ”)
Ex-1007	Google Security Blog, <i>Advanced sign-in security for your Google account</i> , https://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html (Feb. 10, 2011) (“ <i>Google</i> ”)
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	<i>Authentication in an Internet Banking Environment</i> , 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
Ex-1018	Sugata Sanyal, et al., A Multifactor Secure Authentication System for Wireless Payment, <i>in</i> Emergent Web Intelligence: Advanced Information Retrieval, Advanced Information and Knowledge Processing (2010).
Ex-1019	Ali Al-Qayedi et al., <i>Combined Web/Mobile Authentication for Secure Web Access Control</i> , Wireless Communications and Networking Conference, Vol. 2 (Apr. 2004).
Ex-1020	File History for U.S. Patent No. 8,195,576 to Grigg
Ex-1022	Mihai Hulea, <i>Fingerprint Recognition Distributed System</i> , 2008 IEEE International Conference on Automation, Quality and Testing, Robotics (May 2008)
Ex-1023	Shaun Whitehead, <i>IN SAFE HANDS: A review of mobile phone anti-theft designs</i> , European Journal on Criminal Policy and Research (Mar. 2008).
Ex-1024	Engadget, <i>Stick 'em up. A Pantech G1100? Then gimme your phone and your thumbs!</i> , https://www.engadget.com/2004-08-03-stick-em-up-a-pantech-g1100-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, <i>Biometric Security for Cell Phones</i> , Informatica Economică, vol. 13 (Jan. 2009).

IV. LEGAL STANDARDS

21. I am not a lawyer. My understanding of the legal standards to apply in reaching the conclusions in this declaration is based on discussions with counsel for Petitioner, my experience applying similar standards in other patent-related matters, and my reading of the documents submitted in this proceeding. In preparing this declaration, I have tried to faithfully apply these legal standards to the challenged claims.

22. I have been informed that there are two ways in which prior art may render a patent claim unpatentable. First, I have been informed that the prior art can “anticipate” a claim. Second, I have been informed that the prior art can render a claim “obvious” to a person of ordinary skill in the art. I understand that a claim is patentable if it was not anticipated and would not have been obvious by the prior art at the effective filing date of the patent.

23. I have been informed that a dependent claim is a patent claim that refers back to another patent claim. I have been informed that a dependent claim includes all of the limitations of the claim to which it refers.

24. I have been asked to provide my opinions as to whether the cited prior art teaches or renders obvious claims 1-10 of the '347 Patent from the perspective of a person of ordinary skill in the art at the '347 Patent's earliest claimed priority date of July 18, 2011, as described in more detail below.

25. I have been informed that in *inter partes* review proceedings, such as this one, the party challenging the patent bears the burden of proving unpatentability by a preponderance of the evidence. I understand that a preponderance of the evidence means "more likely than not."

26. For purposes of this declaration, I have been asked to provide my opinions on issues regarding unpatentability. I have been informed of the following legal standards, which I have applied in forming my opinions.

A. Level of Ordinary Skill

27. I have been informed a person of ordinary skill in the art is determined by considering several factors, including the (i) type of problems encountered in the art; (ii) prior art solutions to those problems; (iii) rapidity with which innovations are made; (iv) sophistication of the technology; and (v) educational level of active workers in the field. I have been instructed to assume a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors discussed above.

B. Prior Art

28. I have been advised and understand the information used to evaluate whether an invention was new and not obvious when made is generally referred to as “prior art.” I understand that prior art includes patents and printed publications that existed before the earliest claimed priority date or the earliest filing date of the patent (which I have been informed is also called the “effective filing date”). I have been informed and understand that a patent or published patent application is prior art if it was filed before the earliest filing date of the claimed invention and that a printed publication is prior art if it was publicly available before the earliest filing date.

C. Anticipation

29. I have been informed that under 35 U.S.C. § 102, a patent claim is unpatentable for anticipation if it is not novel, including if the claimed subject matter was patented or described in a printed publication before the effective filing date of the claimed invention. I have been informed that this is referred to as unpatentability by anticipation. I have been informed that a patent claim is anticipated under § 102 if a single prior art reference discloses all limitations of the claimed invention.

D. Obviousness

30. I have been informed that under 35 U.S.C. § 103, a patent claim is unpatentable if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains at the time the invention was made. I have been informed that this is referred to as unpatentability by obviousness.

31. I have been informed that a proper obviousness analysis includes the following: (a) determining the scope and content of the prior art; (b) ascertaining the differences between the prior art and the claims at issue; (c) resolving the level of ordinary skill in the pertinent art; and (d) considering evidence of secondary indicia of non-obviousness (if available). I am not aware of any evidence of secondary considerations that would support a determination of non-obviousness of the claimed subject matter in the '347 patent.

32. I have been informed that the relevant time for considering whether a claim would have been obvious to a person of ordinary skill in the art is the time of invention. For my obviousness analysis, counsel for Petitioner instructed me to assume that the date of invention for the Challenged Claims is July 18, 2011. My opinions would not change if I assumed a later date of invention.

33. I have been informed that a reference may be modified or combined with other references or with a person of ordinary skill in the art's own knowledge if the person would have found the modification or combination obvious. I have also been informed that a person of ordinary skill in the art is presumed to know all the

relevant prior art, and the obviousness analysis may take into account the inferences and creative steps that a person of ordinary skill in the art would employ.

34. I have been informed that whether a prior art reference renders a patent claim obvious is determined from the perspective of a person of ordinary skill in the art. I have also been informed that, while there is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, and while a suggestion to combine known elements to achieve the claimed invention may come from the prior art as a whole or individually and may consider the inferences and creative steps a person of ordinary skill in the art would employ, as filtered through the knowledge of one skilled in the art, obviousness grounds cannot be sustained by mere conclusory statements and must include some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.

35. In determining whether a prior art reference could have been combined with another prior art reference or other information known to a person having ordinary skill in the art, I have been informed that the following principles may be considered:

- a. A combination of familiar elements according to known methods is likely to be obvious if it yields predictable results;

b. The substitution of one known element for another is likely to be obvious if it yields predictable results;

c. The use of a known technique to improve similar items or methods in the same way is likely to be obvious if it yields predictable results;

d. The application of a known technique to a prior art reference that is ready for improvement to yield predictable results;

e. Any need or problem known in the field and addressed by the reference can provide a reason for combining the elements in the manner claimed;

f. A person of ordinary skill often will be able to fit the teachings of multiple references together like a puzzle; and

g. The proper analysis of obviousness requires a determination of whether a person of ordinary skill in the art would have a “reasonable expectation of success”—but not “absolute predictability” of success—in achieving the claimed invention by combining prior art references.

36. I have been informed that, when a work is available in one field, design alternatives and other market forces can prompt variations of it, either in the same field or in another. I have been informed that if a person of ordinary skill in the art could have implemented a predictable variation and would have seen the benefit of doing so, that variation is likely to have been obvious. I have been informed that, in

many fields, there may be little discussion of obvious combinations, and in these fields market demand—not scientific literature—may drive design trends. I have been informed that, when there was a design need or market pressure and there are a finite number of predictable solutions, a person of ordinary skill in the art would have had a good reason to pursue those known options.

37. I have been informed that the law permits the application of “common sense” in examining whether a claimed invention would have been obvious to a person skilled in the art. For example, I have been informed that combining familiar elements according to known methods and in a predictable way may suggest obviousness when such a combination would yield nothing more than predictable results. I understand, however, that a claim is not obvious merely because every claim element is disclosed in the prior art and that a party asserting obviousness must still provide a specific motivation to combine or modify the references as recited in the claims and explain why one skilled in the art would have reasonably expected to succeed in doing so.

38. I have been informed that there is no rigid rule that a reference or combination of references must contain a “teaching, suggestion, or motivation” to combine references. But I also understand that the “teaching, suggestion, or motivation” test can be a useful guide in establishing a rationale for combining elements of the prior art. I have been informed that this test poses the question as to

whether there is an express or implied teaching, suggestion, or motivation to combine prior art elements in a way that realizes the claimed invention, and that it seeks to counter impermissible hindsight analysis.

39. I have been informed that, in an obviousness analysis, prior art must be analogous prior art to the patent being considered. I have been informed that a prior art reference is considered to be analogous, or in the same field of art, if the reference is either (1) in the same field of endeavor as the challenged patent, regardless of the problems the challenged patent and the prior art address, or (2) reasonably pertinent to the particular problem being solved by the challenged patent.

V. TECHNICAL BACKGROUND

40. Multi-factor authentication was known in the art before the '347 patent. This authentication requires two or more “factors” from a user, 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/or something the user is (e.g., biometric characteristic, such as a fingerprint, etc.). 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 to financial institutions for any “high-risk transactions involving access to customer information or the movement of funds to other parties.” Ex-1015, 6. By 2011, multi-factor authentication was a well-known and understood way authenticate a user of a mobile device. *See, e.g.*, 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”).

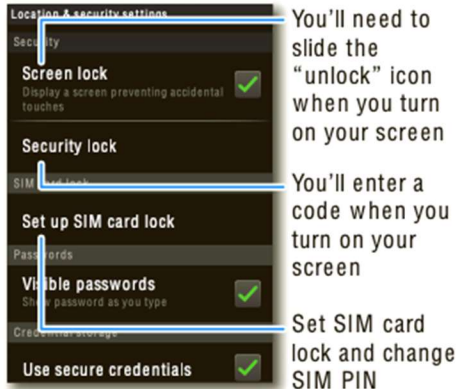
41. Providing a user interface to allow a user to select a setting that requires single or multi-factor authentication before using a feature on a mobile application, as represented in the '347 patent, was not an advance over the prior art. In early 2011, for example, Motorola released the Android ATRIX 4G smartphone that featured a fingerprint reader for authentication and security. *See* Ex-1028, 1. As shown below in its user manual, the ATRIX 4G included a user interface that employed checkboxes for customizing the activation of alternative authentication methods for accessing the device, including drawing a pattern, entering a PIN, entering a password, and using a fingerprint:

Security

Quick Start: Security

Find it: Menu  > **Settings** > **Location & security**

You have lots of ways to keep your phone safe.



If you lose your phone, you can log into your MOTOBLUR account from a computer to locate your phone or clear the data on it: www.motorola.com/mymotoblur.

Screen Lock

To set your security level, touch Menu  > **Settings** > **Location & security** > **Set up screen lock**:

- **Pattern** - draw a pattern to unlock.
- **PIN** - enter a numeric code to unlock
- **Password** - enter a text password to unlock
- **Fingerprints** - swipe your finger across the power key to unlock

Note: You can make emergency calls on a locked phone ("Emergency Calls" on page 9). A locked phone still rings, **but you need to unlock it to answer.**

Ex-1028, 60-62.

42. Beyond fingerprint recognition, other biometric methods for securing and authenticating access to mobile devices were also well known well before the '347 patent. For example, in 2009, Pocovnicu described "biometric security for cell phones" that included the use of voice recognition, face recognition, signature recognition, and keystroke recognition. EX-1029, Title, 61-63.

VI. THE '347 PATENT

A. Overview of the '347 patent

43. The application leading to the '347 patent was filed on August 10, 2021, and claims priority to earlier-filed applications dating back to July 18, 2011.

Ex-1001, Cover, 2. For purposes of this declaration, I have assumed the '347 patent is entitled to claim July 18, 2011, as the date of invention.

44. 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.

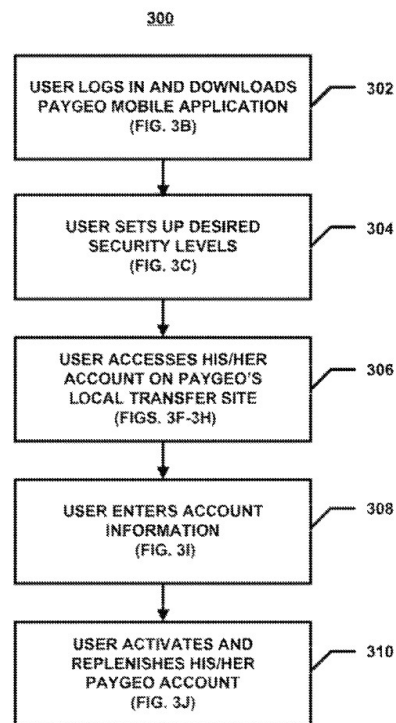


FIG. 3A

Ex-1001, Fig. 3A.

45. After downloading and starting a mobile application, such as a “PayGeo service,” a user may “set[] up the desired security level or levels for the user station 105.” Ex-1001, 4:15-23, 10:32-39. Using a user interface on the mobile application, the user may set “at least one of four security levels,” including a first security level

set by “entering a user-selected password,” a second level set by “recording a voice recognition password, signature, or template,” a third level set by “entering a user-selected fingerprint,” and a fourth level set by “providing a user DNA sample.” Ex-1001, 10:40-53.

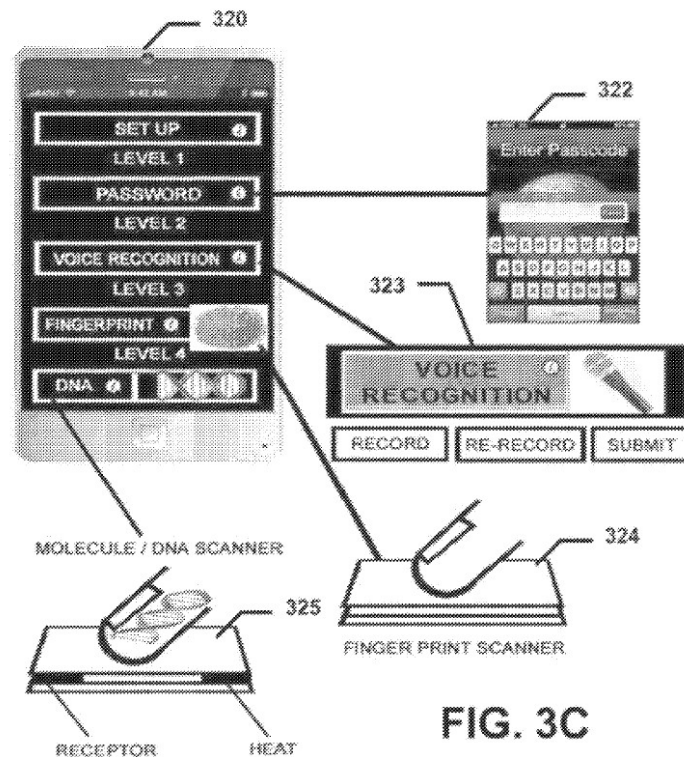


FIG. 3C

Ex-1001, Fig. 3C.

46. The user may then log into the application after “select[ing] the preferred identification 30 security levels that were previously set up at step 304.” Ex-1001, 11:26-41. The user may also elect, via an interface on the mobile application, “to enter alternative or additional security levels as illustrated in FIG. 3H, such as a thumb print 348 or a voice print 350.” Ex-1001, 11:26-41.

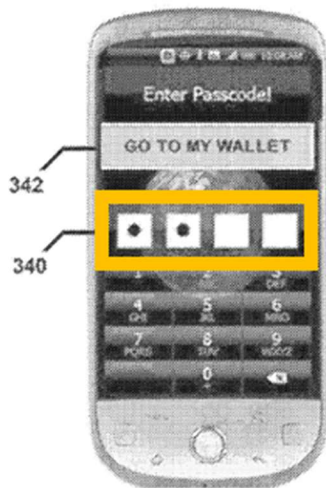


FIG. 3F

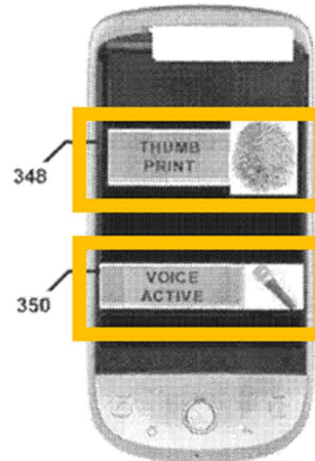


FIG. 3H

Ex-1001, Figs. 3F, 3H (annotating “password 340,” “thumb print 348,” and “voice print 350”).

47. Although the ’347 patent discloses authentication and security of an application for financial transactions, the claims of the ’347 patent focus on user interfaces for setting application security levels for a “local application,” more generally. None of the claims of the ’347 patent recite a financial transaction.

B. Summary of the Prosecution History of the ’347 patent

48. I have reviewed the prosecution history of the application that led to the ’347 patent. *See* Ex-1002. The claims were rejected during prosecution based on references that were deemed not prior art, and the claims were then allowed. *See* Ex-1002, 67-78, 58-61, 15-22, 20 (finding the ’347 patent “predates the earliest filing date” of the references asserted in the Examiner’s office action).

C. Claim Construction of Terms in the '347 patent

49. I have been informed that, for purposes of *inter partes* review, the standard for construction of terms in a patent's claims is the same as that applied in federal district court litigation. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of one of ordinary skill in the art at the time of the alleged invention.

50. I understand that a district court has yet to construe the claim terms of this patent. At this time, I see no need to construe any terms of the challenged claims for the purposes of this proceeding. Accordingly, in preparing my analysis I have applied the ordinary and customary meaning that each claim term would have had to POSITA in light of the '347 patent's specification and prosecution history.

51. If any claim terms are differently construed, I reserve the right to reassess my opinions under those constructions.

VII. PERSON OF ORDINARY SKILL IN THE ART

52. As discussed above, I have been informed that patentability must be analyzed from the perspective of a "person of ordinary skill in the art" in the same field as the patent-in-suit at the time of the invention.

53. I refer to a person of ordinary skill in the art here as a "POSITA." A POSITA in this case 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. Additional relevant work experience can compensate for less education, and vice versa. I at least meet this definition of a POSITA, now and as of the priority date of the '347 patent.

54. I am also familiar with the knowledge of a POSITA as of the priority date of the '347 patent. I am able to opine on how a POSITA would have understood the disclosure and claims of the '347 patent, the disclosures of the prior art, the various motivations to combine the prior art, and what combinations would have been obvious to a POSITA.

VIII. THE PRIOR ART

A. Overview of *Grigg* (Ex-1005)

55. U.S. Patent No. 8,195,576 ("*Grigg*," Ex-1005), as indicated on the face of the reference, was filed before the '347 patent on January 31, 2011, and later issued as a United States Patent on June 5, 2012. I understand *Grigg* is prior art to the '347 patent.

56. *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 allowing a transaction to proceed at a point-of-sale location. *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 "instructions" entered by a user, including embodiments in which a transaction amount determines whether user authentication is required. *E.g.*, *Grigg*,

6:37-62. The system determines when a user is engaging in a transaction at a point-of-sale location and then 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.

57. In addition to one or more active authentication methods for a single user, *Grigg* discloses an embodiment requiring authentication by more than one individual before permitting a financial transaction: "[f]or example, ***a couple*** may decide that for transaction amounts greater than \$200 authentication ***by both individuals*** is required." *Grigg*, 6:51-53.

58. *Grigg* also discloses exemplary user interfaces for setting 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 includes "the types of security features 906 that are uploaded to the financial transaction security system for that user." *Grigg*, 18:17-50, Fig. 9. The interface 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.

59.

FIG. 9

Grigg, Fig. 9 (annotating the “ACTIVE” authentication methods).

60. In my opinion, both *Grigg* and the '347 patent are from the same field of endeavor: application security to protect a user's sensitive information. Like the '347 patent, *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.

B. Overview of *Carter* (Ex-1006)

61. U.S. Patent Application Publication No. 2009/0152343 ("*Carter*," Ex-1006), published on June 18, 2009, before the '347 patent. I understand *Carter* is prior art to the '347 patent.

62. Like *Grigg*, *Carter* discloses methods for authenticating a user using a mobile device to conduct a transaction. *Carter*, Abstract, ¶¶5-8. *Carter* discloses the "difficulty in reliably authenticating transactors electronically," which "creates the danger of fraud" in financial transactions. *Carter* ¶3. 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* ¶¶7, 31-40. *Carter* discloses that its mobile device is "configured for multi-factor authentication of transactions" and discloses "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* ¶¶31-32.

C. Overview of *Google* (Ex-1007)

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

of the article and as cataloged by the Internet Archive the day *Google* posted (February 10, 2011). Ex-1021 ¶¶1-7. I am aware of the Internet Archive and its goal of building a digital library of Internet websites. *See* The Wayback Machine, <https://web.archive.org/> (“The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form.”). In my opinion, *Google* would have been publicly available and accessible to POSITAs via the Internet on the date of its publication, which was before the ’347 patent was filed. I understand that *Google* qualifies as prior art to the ’347 patent.

64. 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.” *Google*, 1. This information may include “[y]our Gmail account, your photos, your private documents.” *Google*, 1.

65. 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. According to *Google*, “2-step verification

requires two independent factors for authentication ... : your password, plus a code obtained using your phone.” *Google*, 1.

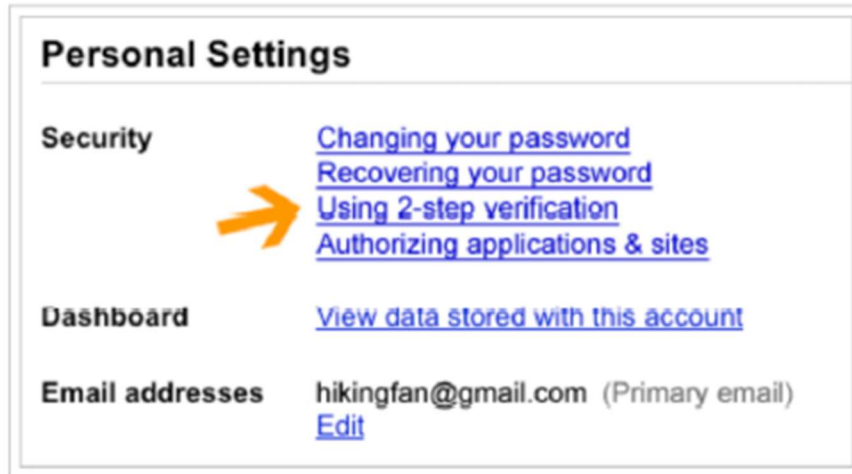
66. Authentication for a *Google* Account is a prerequisite to using certain *Google* applications, including Gmail. Ex. 1014, 30:61-65 (discussing the use of “a Google account for accessing one or more web based services such as Gmail, Google calendars, Google reader, etc.”).

67. Once authenticated, Gmail can be accessed on a mobile device in at least two different ways:

68. First, a user may launch an Internet browser on a mobile device and access Gmail via Gmail’s mobile website. Ex-1008, ¶22 (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.

69. Second, a user may download a standalone Gmail application on a mobile device. 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.

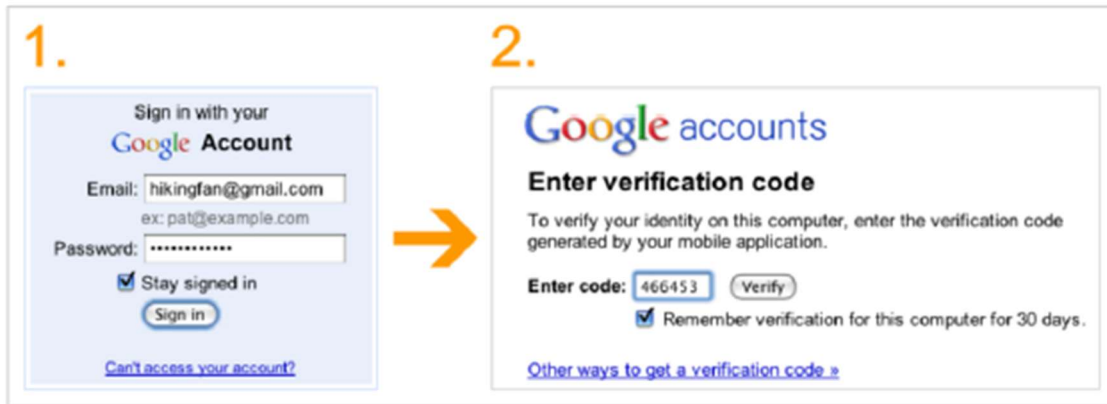
70. *Google* explains that security for accessing a *Google* Account can be adjusted using the following user interface:



Google, 1.

71. From this “Account Overview” interface, a user can elect to opt-in to 2-step verification or continue with simply a username/password. *Google*, 1. 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.

72. 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.” *Google*, 1. The interfaces for the username/password and verification code are shown below:



Google, 1.

73. *Google* is analogous art to the '347 patent. Both *Google* and the '347 patent are from the same field of endeavor: application security to protect a user's sensitive information. Like the '347 patent, *Google* provides user interfaces that enable a user to improve the security associated with applications containing sensitive information by opting-in to a multi-layered approach to authentication.

Google, 1; Ex-1001, Abstract, 10:32-53.

IX. OPINIONS ON UNPATENTABILITY

74. The following prior art, in my opinion, anticipates and/or renders obvious claims 1-10 of the '347 patent:

Ground	Claims	Basis	Prior Art
1A	1-10	Anticipation	<i>Grigg</i>
1B	1-10	Obviousness	<i>Grigg</i>
2	1-10	Obviousness	<i>Grigg and Carter</i>

Ground	Claims	Basis	Prior Art
3A	1, 2, 6, 7	Anticipation	<i>Google</i>
3B	1, 2, 6, 7	Obviousness	<i>Google</i>
4	3-5, 8-10	Obviousness	<i>Google and Carter</i>

A. Ground 1A and 1B: *Grigg* Anticipates and/or Renders Obvious Claims 1-10

1. Claim 1

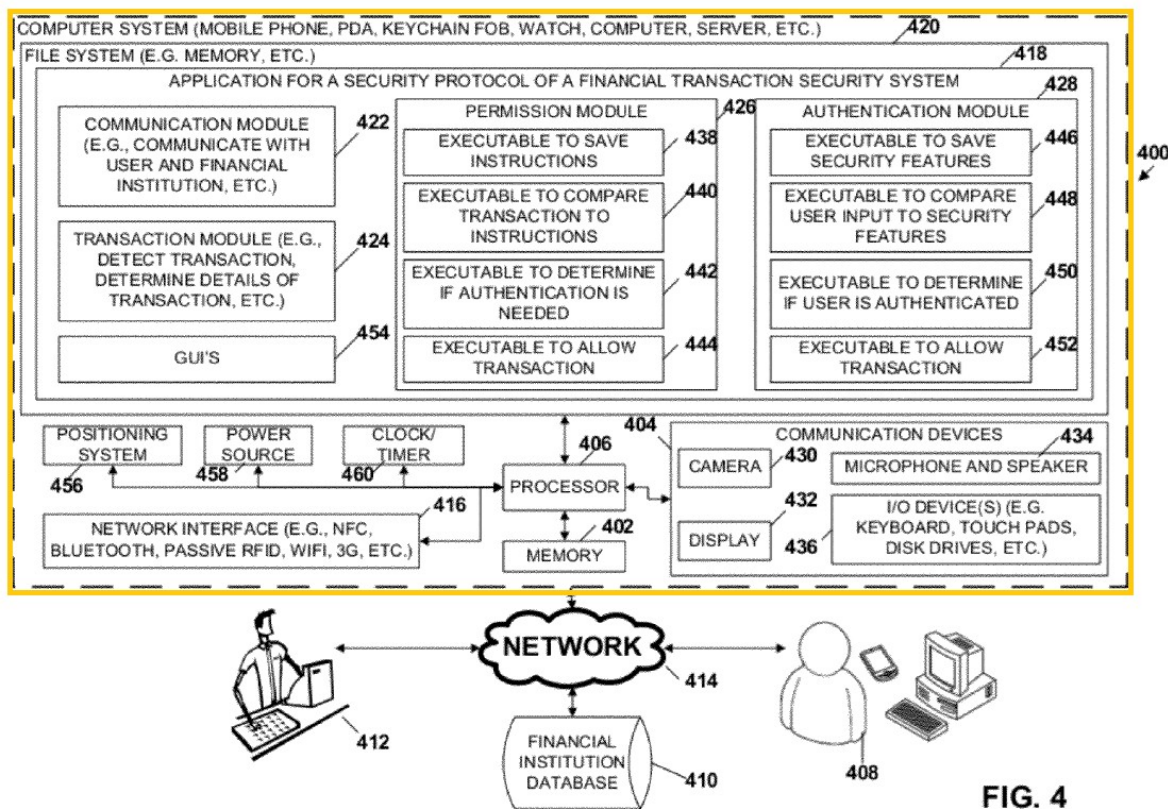
- a. [1pre] “A method of securely accessing a local application on a mobile device, comprising the steps of:”

75. *Grigg* discloses a method of securely accessing a local application on a mobile device.

76. **Mobile device:** *Grigg* refers to its mobile device as a mobile wallet, electronic wallet, or financial transaction security system. *Grigg*, 1:48-56, 1:57-2:3, 2:4-3:41, 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 (“smartphone or PDA that allows a user to enter into transactions using the smartphone or PDA”), 12:35-49 (system 400 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”).

77. *Grigg*’s 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.



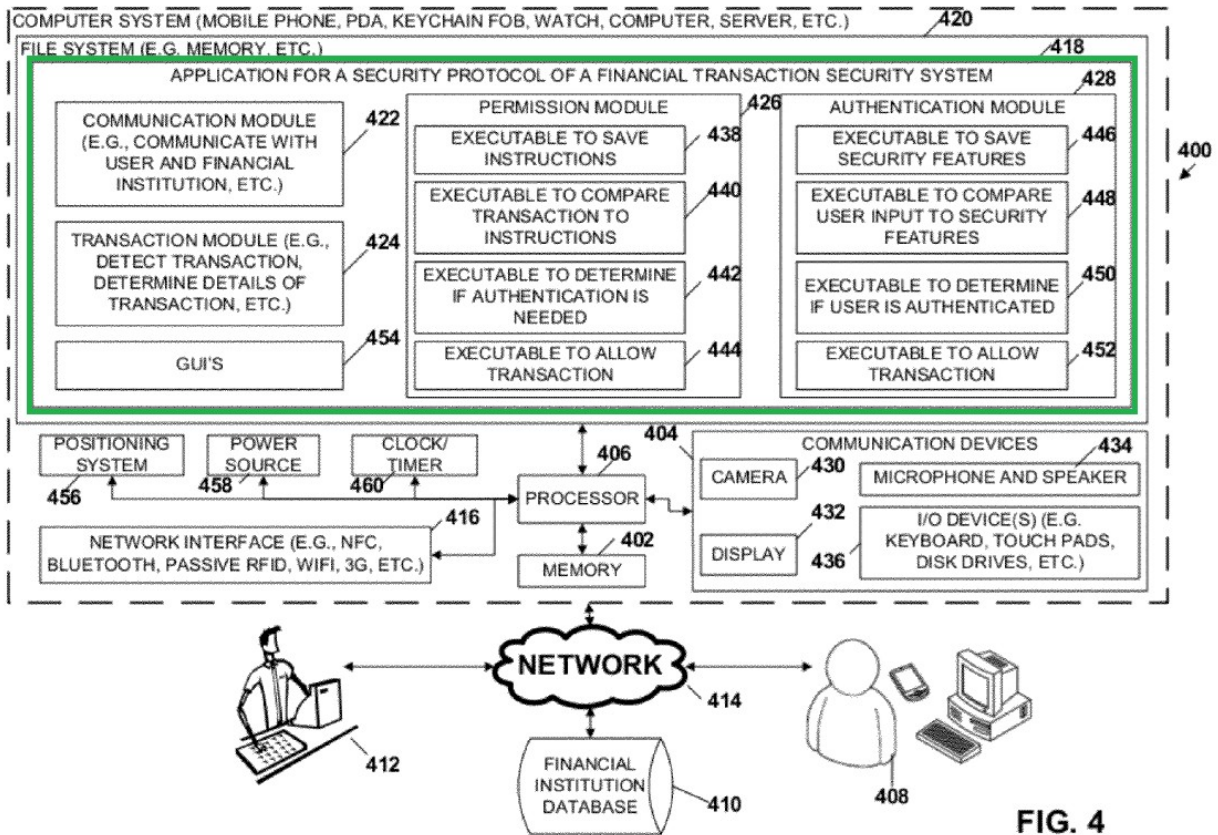
Grigg, Fig. 4 (annotating system 400), 12:35-40 (“In some embodiments, the system 400 includes a computer system such as a mobile phone, PDA, keychain fobs, watch, computer, server, electronic device, etc.”).

78. In my opinion, *Grigg*'s financial transaction security system, implemented for example as a mobile phone, smartphone, PDA or the like, is a "mobile device," as claimed.

79. **Local application on the mobile device:** *Grigg* discloses that a user 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 (disclosing "an application on a smartphone ... [that] stores the user's security protocol, determines that the user is conducting a transaction at a point-of-sale device, and compares the transaction with the instructions provided by the user"), 6:14-28 (receiving the security protocol "through a software application"). *Grigg*'s mobile device application discloses a "local application" on its mobile device.

80. *Grigg*'s mobile device application, which *Grigg* refers to as a "security protocol application 418," includes a permission module and an authentication module. *Grigg*, 13:11-65, Fig. 4. The security protocol application 418 "allows for communication between a communication module 422, a transaction module 424, a permission module 426, and an authentication module 428 to send, receive, and store information related to the financial transaction security system, determine details relating to a transaction, determine whether user authentication is not necessary, and authenticate the user's identity." *Grigg*, 13:16-24. The security protocol application 418 includes "Graphical User Interfaces (GUIs) 454" that assist the user in

“utilizing ... any ... feature of the financial transaction security system 400.” *Grigg*,
15:15-23, Fig. 4.



Grigg, Fig. 4 (annotating *Grigg*'s mobile device application in security protocol application 418).

81. A POSITA would have understood *Grigg*'s security protocol application 418 is the same mobile device application *Grigg* references elsewhere in its disclosure, including Figures 1-3.

82. In each of these embodiments, for example, *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.

83. In my opinion, *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.

84. **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 at a point-of-sale location. *See* Element [1d] (Grounds 1A and 1B); *see Grigg*, Abstract (“[T]he system requests input from the user, compares the input to the security feature, and determines if the user is authenticated. The user is able to customize both the instructions and the security features to provide greater control over financial transaction security.”), 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.

85. *Grigg*’s methods of authenticating a user using its mobile device application, as further explained below, discloses “[a] method of securely accessing” the local application on the mobile device, as claimed.

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

86. In my opinion, *Grigg* discloses launching its local application on its mobile device.

87. 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.

88. To enter the security protocol, *Grigg* discloses that "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 "initiate[d]" in this example is *Grigg*'s mobile device application or security protocol application 418 because *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. *Grigg*, 4:48-64; 6:14-28, 13:11-24.

89. *Grigg* therefore discloses "launching" a local application on the mobile device, in my opinion.

- 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;"**

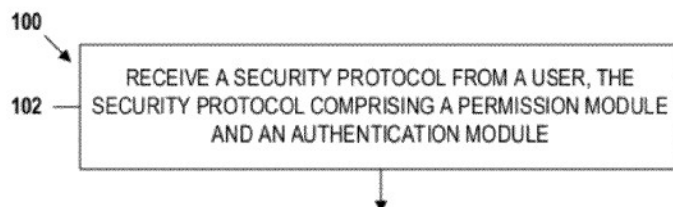
90. In my opinion, *Grigg* discloses or at a minimum renders obvious Element [1b].

91. **Enabling a user to set a desired security level configuration setting in the local application for the mobile device:** *Grigg*'s mobile device application,

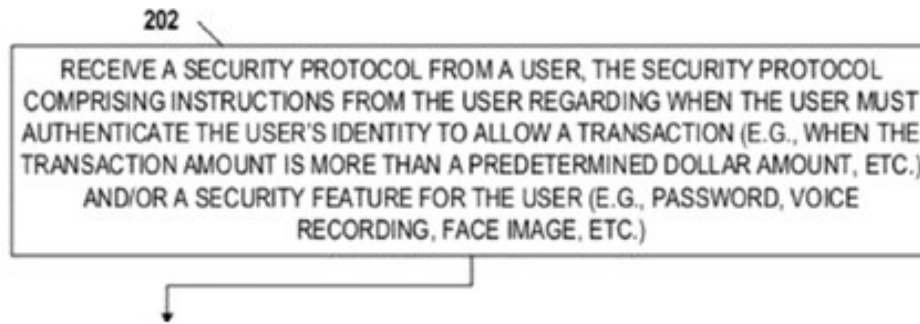
including security protocol application 418, enables a user to customize “security protocols” for transactions at a point-of-sale location. *Grigg*, 1:57-60, 2:4-7, 3:10-14, 3:27-32.

92. 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,” who may “change the security protocol in the same manner or in a different manner from which the protocol was initially established.” *Grigg*, 4:48-63; *see also Grigg*, 5:29-31 (describing the “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).

93. Receipt of the user’s chosen method(s) of authentication by *Grigg*’s system is further illustrated in the process flow diagrams of Figures 1 and 2:



Grigg, Fig. 1 (cropped).



Grigg, Fig. 2 (cropped).

94. In my opinion, this discloses “enabling a user to set a desired security ... configuration setting,” as claimed.

95. *Grigg* discloses that its security protocol “is saved in a mobile device of the user.” *Grigg*, 8:55-9:11. An authentication module of the mobile device “includes the security features provided by the user.” *Grigg*, 4:64-5:11. Before allowing the user to perform a transaction, the system compares user input, such as a voice command, facial scan, etc., to the stored security features “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. *Grigg* thus uses these stored security features to authenticate a user. *See Grigg*, 10:58-11:32, 11:43-12:25, 13:16-24, Figs. 3, 4.

96. As disclosed by *Grigg*’s claim 13, requesting authentication of the user’s identity may comprise receiving input of one or more of the stored security features: “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 (claim 13).¹

97. In my opinion, *Grigg* thus discloses authenticating a user by a “single” or a “plurality” of authentication methods.

98. *Grigg* also discloses an exemplary interface for enabling a user to enter its security features.

99. For example, 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. This 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. The user can configure the authentication module with “at least one security feature.” *Grigg*, 6:21-23, 20:63-65 (claims 2, 3).

100. As shown below in annotated Figure 9, interface 900 indicates at least two of seven potential authentication methods that are concurrently active. The active authentication methods are facial scan 910 and voice scan 912, which are each

¹ As *Grigg*’s file history indicates, claim 13 of *Grigg* was filed as original claim 20 in the application leading to *Grigg* and thus forms part of *Grigg*’s original disclosure. Ex-1020, 214-220.

shown in a state where they are “ACTIVE.” *Grigg*, Fig. 9. The other available (but not stored) methods are challenge question 916, iris scan 922, fingerprint scan, and custom device security feature 924. *Grigg*, Fig. 9.

900

FINANCIAL TRANSACTION SECURITY SYSTEM 502 902

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

904 CURRENT USER: XXXXX 906 CLEAR

908 USERNAME: XXXXX EDIT 914

PASSWORD: ***** EDIT

916 CHALLENGE QUESTION: NOT SELECTED ADD 920

910 FACIAL SCAN: IMAGE STORED AND ACTIVE EDIT 920

912 VOICE SCAN: VOICE RECORDING STORED AND ACTIVE EDIT

922 IRIS SCAN: NOT SUPPORTED 928

918 FINGERPRINT SCAN: FINGERPRINT NOT SAVED ADD

924 CUSTOM DEVICE SECURITY FEATURE: NOT SUPPORTED

926 CHANGE CURRENT USER

FIG. 9

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

101. In my opinion, a POSITA would have understood from *Grigg*’s Figure 9 that the username and password, facial scan, and voice scan security features are stored on *Grigg*’s mobile device. A POSITA further would have understood that at least the facial scan 910 and voice scan 912 are active because

Figure 9 indicates these two authentication methods as currently “ACTIVE,” while username and password is available but not “ACTIVE.”

102. In my opinion, a POSITA also would have understood from *Grigg*’s disclosure of (1) allowing a user to configure a security module within security protocol application 418, including requiring authentication by a user by “at least one” security feature; and (2) indicating which features are “ACTIVE” via interface 900, that a user may set a desired security level configuration setting in the local application for the mobile device. Indeed, *Grigg* expressly discloses authenticating its user “in a variety of ways” based on the security features. *Grigg*, 10:66-11:23. In embodiments, an authentication request “allows a user to authenticate his identity in any manner” or “in a specific manner.” *Grigg*, 10:66-11:23.

103. In my opinion, *Grigg* therefore discloses authenticating a user by one stored and “ACTIVE” authentication method (e.g., security feature) or by more than one stored and “ACTIVE” authentication method.

104. **The desired security level configuration setting establishing whether the local application requires a single security level or a plurality of security levels**: In my opinion, *Grigg* discloses or at least renders this feature obvious.

105. As discussed, *Grigg* discloses that the user can configure the authentication module with more than one security feature *Grigg*, 6:21-23 (“at least

one security feature”), cl. 2 (same), 3 (same). *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. The user may further “set different ***tiers*** of authentication depending on the transaction amount.” *Grigg*, 10:66-11:23. This includes setting “levels” where authentication may or may not be required. *Grigg*, 7:56-60 (“In other embodiments, the user sets ***different levels of security*** required in different categories.”), 8:31-41 (“By adjusting the ***security levels*** based on user information, the user is able to customize the ***security levels***, assist in budgeting, and gain greater control over expenses.”), 6:45-61 (“tiered levels”).

106. In addition, as discussed above, *Grigg* expressly discloses receiving one or more security features to authenticate a user. This includes requiring “at least one” security feature (e.g., one or more) before permitting a transaction. *Grigg*, 21:58-62 (claim 13); *see also Grigg*, 6:45-61 (contemplating requiring “***different types of authentication***”). *Grigg* further contemplates receiving security features from multiple users: “a couple may decide that for transaction amounts greater than \$200 ***authentication by both individuals is required.***” *Grigg*, 6:45-61.

107. *Grigg* therefore discloses allowing the user to require one or more authentication methods (e.g., “security features”) before a transaction may commence, which discloses a user setting a “security level configuration setting”

that establishes “a single security level or a plurality of security levels before allowing access to at least a feature in the local application.”

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

109. For example, it would have been obvious to a POSITA to modify *Grigg* to enable a user to select between a single and multiple “ACTIVE” security features and thus apply a different “tier” or “level” of authentication before authorizing a transaction at a point-of-sale location.

110. A POSITA would have found it obvious, for example, to modify interface 900 to enable a user to “edit 914 ... stored [security] features using the mobile device” and separately enable them as “ACTIVE” according to Figure 9. *See Grigg*, 18:22-30, Fig. 9.

111. 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 based on user preference for desired security.

112. This modification would have been an obvious, in my opinion, 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, permitting more than one “ACTIVE” security feature, and its contemplated use receiving “at least one” user input to authenticate the user’s identity. *See, e.g., Grigg*, 6:45-61, 7:56-60, 8:31-41, 10:66-11:23, 21:58-61 (claim 13), Fig. 9.

113. In my opinion, a POSITA would have been motivated to modify *Grigg* in this way for several reasons.

114. For example, this 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 (“The financial transaction security system provides numerous opportunities for the user to **customize** security protocols relating to financial transactions conducted through mobile devices.”), 1:48-56 (disclosing that a user may “**customize** payment procedures and authentication protocols”), 2:46-49 (same), 5:29-31 (same), 8:31-41 (same), 8:49-55 (same).

115. As *Grigg* recognizes, a user may desire to apply more security to certain transactions while convenience may be more important for others. *See, e.g., Grigg*, 1:8-14 (describing users 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]”).

116. Satisfying one of *Grigg*'s dual desires, modifying *Grigg* to enable a user to select more than one active security feature would have improved the security of *Grigg*'s mobile wallet during a transaction. By allowing a user to set more than one authentication method as "ACTIVE" (e.g., a password *and* biometric information) via interface 900, transaction security would be improved by requiring additional authentication methods from the user. This would have given additional certainty to a mobile device user that a transaction will not proceed unless the user is who he or she purports to be.

117. Providing this capability would have reduced potential fraud during transactions in *Grigg* by requiring, for example, something a user knows (e.g., a password) and something that is unique to the user (e.g., biometric data), thus reducing the likelihood of unauthorized use of *Grigg*'s mobile wallet. Indeed, POSITAs understood that additional (and distinct) authentication methods are effective in reducing illicit transactions that, for example, may only require one authentication method (e.g., only a user's password or passcode). *See* Ex-1015, 3 ("Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods"); Ex-1017, 1:54-64 ("Even two factor authentication can virtually eliminate fraudulent transactions"); Ex-1016, 2:21-24. This is particularly true for biometric authentication at a point-of-sale location, which is more difficult to fake with a merchant or others customers present.

Modifying *Grigg*'s interface 900 to allow selection of more than one "ACTIVE" security feature thus would have improved security in *Grigg*.

118. Users may alternatively desire convenience during transactions, as *Grigg* recognizes. *See, e.g., Grigg*, 1:8-14, 1:35-41, 6:38-61. Enabling a user to set only one "ACTIVE" authentication method, e.g., a username and password, would have fulfilled this separate goal by reducing the necessary steps to perform a transaction. This would have enabled "ease" and "speed" of the transaction, as *Grigg* contemplates. *See Grigg*, 8:42-55. A POSITA would have benefited from this option, for example, when using the mobile device for low-cost transactions. This would have provided a user with the customization and control that *Grigg* additionally contemplates. *See Grigg*, 1:8-14, 1:35-41, 1:48-56, 7:38-41, 8:18-55.

119. In my opinion, applying an option for multi-factor authentication to *Grigg*'s mobile wallet would have been well-within the capabilities of a POSITA because multi-factor authentication was well-known and accepted in the art, including use with mobile devices applications. Ex-1015, 3; Ex-1016, 2:21-24; Ex-1017, 1:54-64; Ex-1018, Abstract, 344-349; Ex-1019, 1. Modifying *Grigg* in this manner would have involved nothing more than combining *Grigg*'s disclosed security features and multiple tiers or levels of security (including requiring "at least one" security feature) in understood ways. *See Grigg*, 21:58-62 (claim 13). 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.

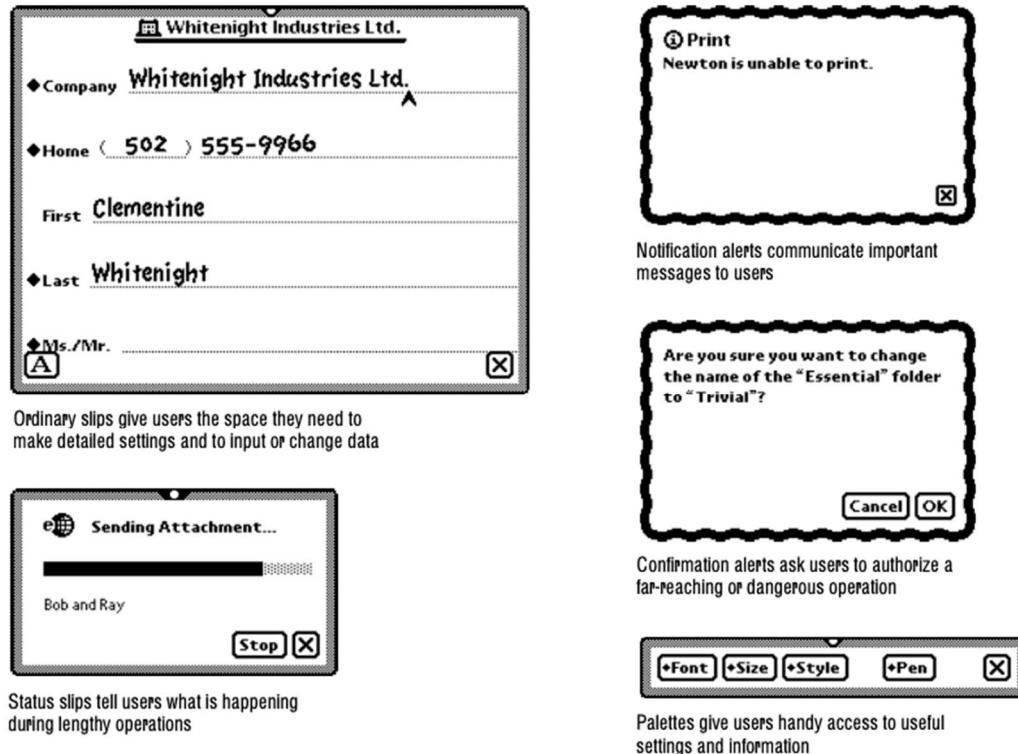
120. In my opinion, modifying *Grigg* in this way also would have given a user greater clarity as to which security feature or features are active for a transaction when more than one are loaded and available.

121. A POSITA would have modified *Grigg* by providing an option with interface 900’s “edit 914” feature to load the security feature and activate it. For example, a POSITA would have understood *Grigg*’s edit 914 provides a menu or window from which a user can load security features. *See Grigg*, 18:17-50, Fig. 9. In my opinion, it would have been obvious when a user clicks on edit 914 to provide the option to load the security feature *and* select whether that security feature was activated or not. Submenus and drill-down windows like this were well-known and ubiquitous in graphical user interfaces since at least the early 1980s, and similar methods have been available on mobile devices since at least the mid 1990s:

Auxiliary Views

When an application needs to display and input more information than will fit in its main view, it displays an auxiliary view. There are several types of auxiliary views, as shown in Figure 2-13 and detailed in the following sections.

Figure 2-13 Examples of auxiliary views



Ex-1026, 46-69.

122. After activating one or more security features within the menu of edit 914 (as modified), interface 900 would indicate which feature is “ACTIVE” and which are not, as *Grigg* shows in Figure 9:

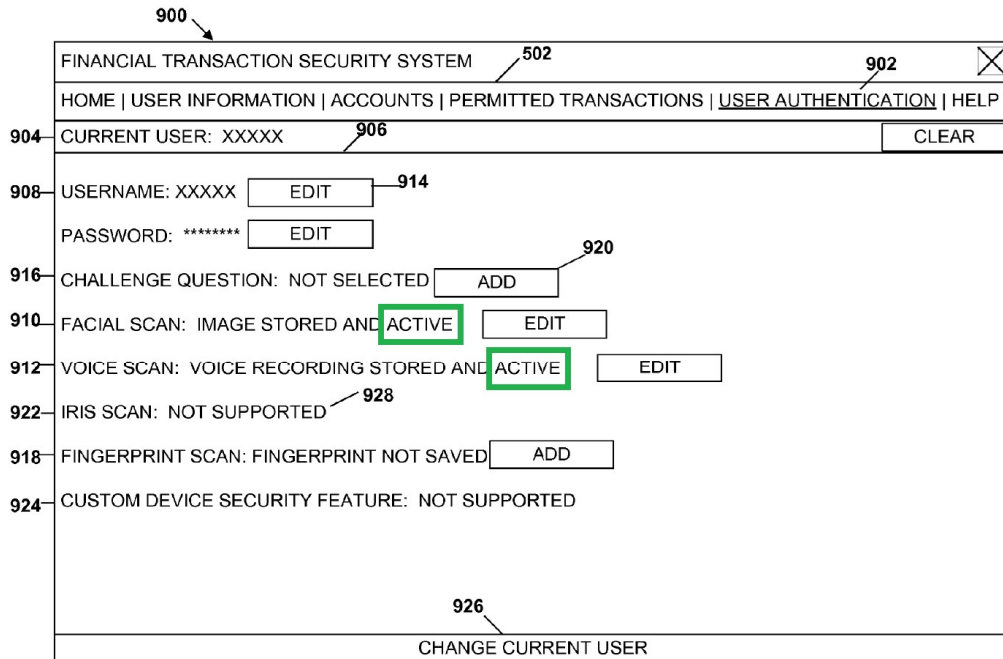


FIG. 9

Grigg, Fig. 9 (annotating “**ACTIVE**” security features).

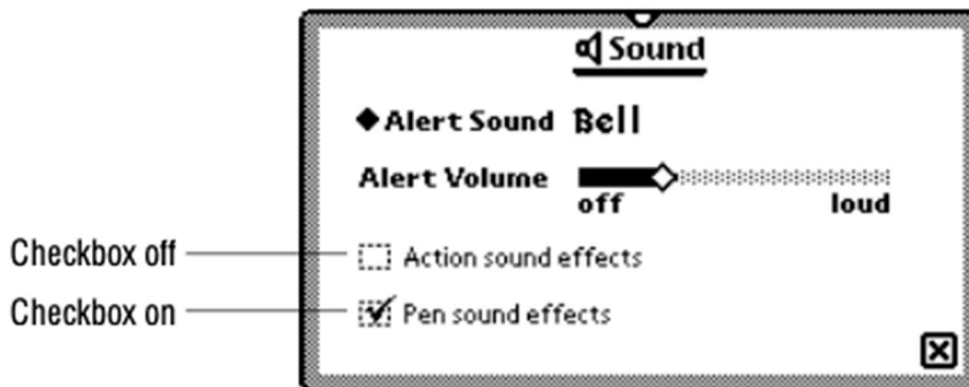
123. Alternatively, it would have been obvious to modify *Grigg* to include an optional activation checkbox or selectable button in interface 900 to select whether a security feature is active or not. Selectable GUI features like this were well-known and ubiquitous in user interfaces since at least the early 1980s, and checkbox controls were similarly ubiquitous on mobile devices since at least the mid 1990s. Ex-1026, 112 (“Checkboxes, like radio buttons, provide alternative choices for users ... Checkboxes act like toggle switches, which can be on or off.”)

Checkboxes

Checkboxes, like radio buttons, provide alternative choices for users. A checkbox is a small dotted box that may include a check mark (✓). It is labeled to the right or left with a word or phrase. Use a checkbox to indicate an option that must be either off or on.

The user selects or deselects the checkbox by tapping it or its label. When the option is selected, a check mark appears in the box. When the option is not selected, the box is empty. Checkboxes act like toggle switches, which can be on or off. A checkbox is on when it is selected and off when it is not selected. Figure 3-18 shows some typical checkboxes.

Figure 3-18 Each checkbox can be on or off



Ex-1026, 112, 113.

124. In *Grigg*'s Figure 9, facial scan 910, voice scan 912, and user name and password have loaded security features by virtue of their respective "edit" boxes being shown. *See Grigg*, Fig. 9. In my opinion, it would have been obvious to include an additional option to select which security feature is active by a selectable checkbox, where modified Figure 9 below shows a facial scan 910 and voice scan 912

enabled and “ACTIVE,” while username and password 908 is not enabled and not indicated as “ACTIVE.”

900

FINANCIAL TRANSACTION SECURITY SYSTEM 502 902

HOME | USER INFORMATION | ACCOUNTS | PERMITTED TRANSACTIONS | USER AUTHENTICATION | HELP

904 CURRENT USER: XXXXX 906 CLEAR

908 **ACTIVE**

916 ☐ USERNAME: XXXXX 914 EDIT

916 ☐ PASSWORD: ***** EDIT

910 ☐ CHALLENGE QUESTION: NOT SELECTED 920 ADD

912 ☒ FACIAL SCAN: IMAGE STORED EDIT

922 ☒ VOICE SCAN: VOICE RECORDING STORED EDIT

918 ☐ IRIS SCAN: NOT SUPPORTED 928

924 ☐ FINGERPRINT SCAN: FINGERPRINT NOT SAVED ADD

CUSTOM DEVICE SECURITY FEATURE: NOT SUPPORTED

926 CHANGE CURRENT USER

FIG. 9

Grigg, Fig. 9 (annotated with selectable checkboxes to activate or deactivate security features).

125. In my opinion, 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. *See, e.g.*, Ex-1026, 46-69, 112, 113. These modifications would have been well within a POSITA’s capabilities and fulfilled *Grigg*’s disclosure that contemplates

receiving input of at least one security feature. *See Grigg*, 21:58-62 (claim 13). This also would have been consistent with *Grigg*'s emphasis on flexibility and user-customization. *See Grigg*, 8:42-55.

126. **Before allowing access to at least a feature in the local application:**

In my opinion, *Grigg* discloses that its authentication module compares user input to the stored security features to authenticate a user before enabling the mobile wallet to perform 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.

127. Allowing a transaction to proceed is a “feature” of *Grigg*'s security protocol application 418. 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.

128. In my opinion, *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.

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

129. In my opinion, *Grigg* discloses “launching the local application after the setting of the desired security level configuration setting.”

130. 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 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.

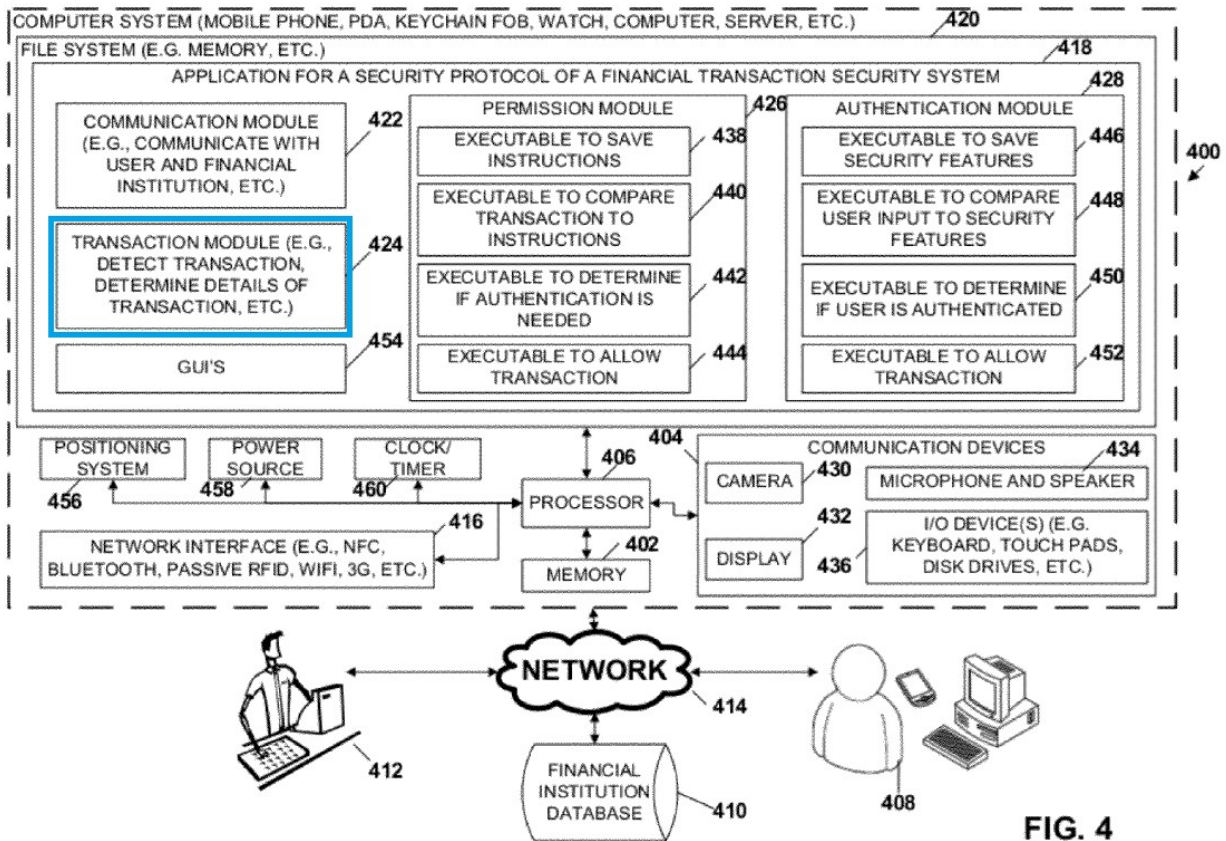


FIG. 4

Grigg, Fig. 4 (annotating [transaction module 424](#)).

131. 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.

132. In my opinion, 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 is set. 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.

133. In my opinion, *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.

134. *Grigg* thus discloses “launching the local application after the setting of the desired security level configuration setting,” as claimed.

- 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.”**

135. In my opinion, *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.

136. In my opinion, *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.”

137. **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 (“If the user has successfully authenticated his identity, in some embodiments the system transfers the user’s financial account information 316.”); *see also Grigg*, 10:50-57, 15:5-14.

138. Before a transaction may proceed, the mobile device compares “instructions” stored in a permissions module to determine what user authentication (if any) is required for a given transaction. *Grigg*, 4:64-5:48. The mobile 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 (“[T]he system determines whether the user must authenticate the user’s identity based on the comparison of the details of the transaction with the instructions.”); *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 (“The system 100 compares 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.

139. *Grigg*’s requiring authentication before allowing the transaction to proceed, including comparing user input to stored security features, discloses the claimed 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.

140. **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**: In my opinion, *Grigg* discloses or at least renders this feature obvious.

141. 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.

142. For a plurality of security level scans, as discussed for Element [1b], *Grigg* discloses or at least renders this obvious. 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. In my opinion, both of these embodiments disclose a plurality of security scans based on the security level configuration setting set by the user.

143. 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. In my opinion, this modification renders obvious a plurality of security scans based on the security level configuration setting set by the user. 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].

144. 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 security level scan or a plurality of security level scans before a transaction may proceed. *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 “for conducting financial transactions with ease,

security, and speed”), 16:63-65 (same), 10:66-11:23 (authentication “can occur in a variety of ways,” including any “specific manner” as defined by the user including setting “different tiers of authentication depending on the transaction amount”).

145. In my opinion, a POSITA would have been motivated to modify *Grigg* in this way to improve security of *Grigg*’s mobile wallet during a transaction for the reasons discussed for Element [1b], including improving security of *Grigg*’s mobile wallet during a transaction, allowing flexibility to require less security when desired, and providing clarity as to which security features are enabled for a transaction. *See* Element [1b].

146. *Grigg* therefore discloses or at least renders Element [1d] obvious.

2. Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”

147. In my opinion, *Grigg* discloses a single security level scan that includes a request for a password.

148. 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 (same), 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:

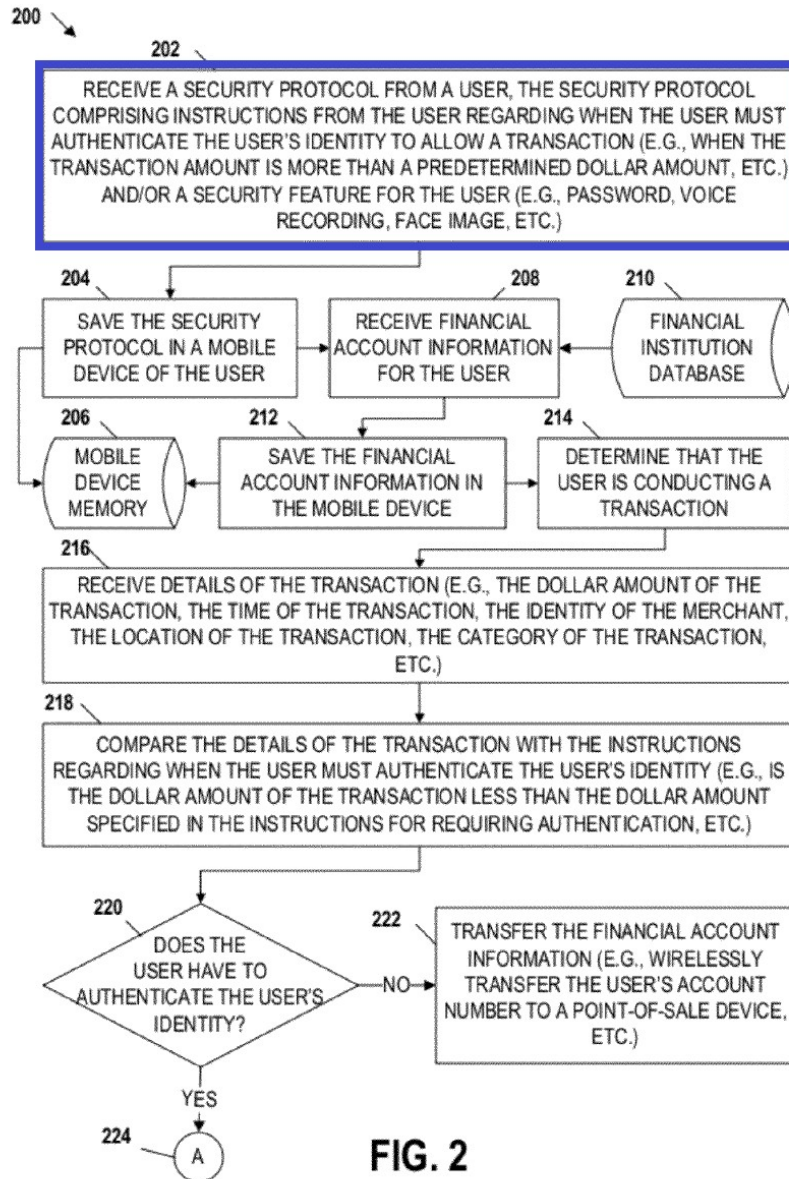


FIG. 2

Grigg, Fig. 2 (annotating 202).

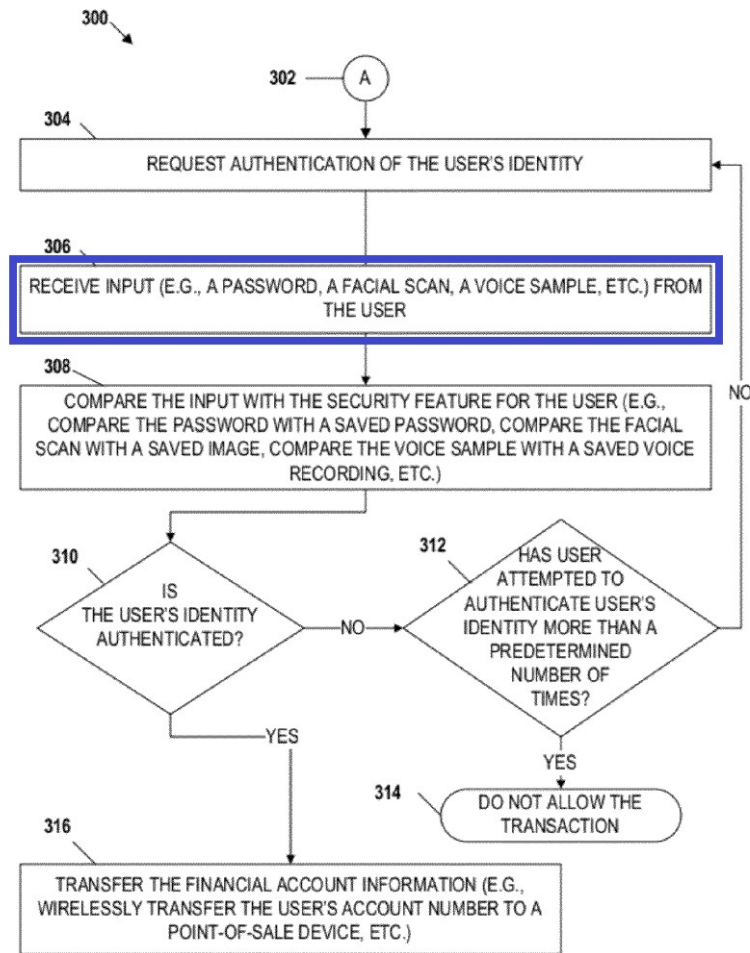


FIG. 3

Grigg, Fig. 3 (annotating 306).

149. *Grigg*'s requirement of a username and password is a single security level scan that "includes a request for a password."

150. In my opinion, *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. *See* Elements [1b], [1d].

3. Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”

151. In my opinion, *Grigg* discloses or at least renders obvious a plurality of security level scans that “includes a biometric scan.”

152. 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 (“biometric scan for amounts greater than \$100”), 11:11-23 (same). *Grigg*’s biometric scans include “a voice sample, a facial scan, a fingerprint scan, [and] an iris scan.” *Grigg*, 2:54-59, 11:24-32 (same), 11:43-12:19 (same), 14:52-15:4 (same), 18:30-40 (same), 20:66-21:2 (claim 4), 21:58-62 (claim 13). This is further shown in the process flow diagram below:

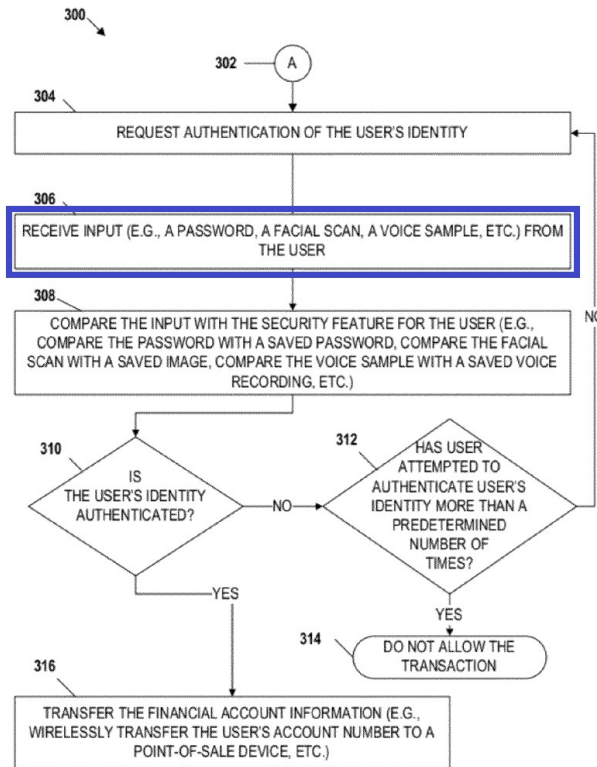


FIG. 3

Grigg, Fig. 3 (annotating 306).

153. 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. *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 at the point-of-sale location. *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.

154. In my opinion, *Grigg* therefore discloses or at least renders obvious claim 3.

4. Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”

155. In my opinion, *Grigg* discloses the biometric scan includes a voiceprint.

156. As discussed for claim 3, *Grigg* discloses that its security features to authenticate a user may include a “biometric scan.” *Grigg*, 6:45-61 (“biometric scan for amounts greater than \$100”), 11:11-23 (same). *Grigg*’s biometric scan may include a “voice sample.” *Grigg*, 2:54-59, 11:24-32 (same), 11:43-12:19 (same), 14:52-15:4 (same), 18:30-40 (same), 20:66-21:2 (claim 4), 21:58-62 (claim 13).

157. As one example of a biometric scan, *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”), 11:43-54 (storing security features that include “voice recordings for use with voice recognition software”), 12:20-25 (prompting the user to “authenticate his identity using a voice scan”), 14:42-45 (“the executable to compare the input to the security features 448 may include voice recognition software to compare the voice sample to a saved voice recording”).

158. A POSITA would have understood that *Grigg*’s “voice sample” that is used to authenticate a user is the claimed “voiceprint” because these are synonymous

terms for a biometric identifier that is based on the individual characteristics of a person's voice. 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").

159. *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. *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. *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.

160. In my opinion, *Grigg* therefore discloses or at least renders obvious claim 4.

5. Claim 5: "The method of claim 3, wherein the biometric scan includes a thumbprint."

161. In my opinion, *Grigg* discloses the biometric scan includes a thumbprint.

162. As discussed for claim 3, *Grigg* discloses that its security features to authenticate a user may include a "biometric scan." *Grigg*, 6:45-61 ("biometric scan

for amounts greater than \$100”), 11:11-23 (same). *Grigg*’s biometric scan may include a “fingerprint scan.” *Grigg*, 2:54-59, 11:24-32 (same), 11:43-12:19 (same), 14:52-15:4 (same), 18:30-40 (same), 20:66-21:2 (claim 4), 21:58-62 (claim 13).

163. *Grigg*’s mobile device “compare[s] ... the fingerprint scan with the previously stored image of the user’s fingerprint” to authenticate a user before allowing a transaction. *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”).

164. A POSITA would have understood that *Grigg*’s “fingerprint” that is used to authenticate a user discloses the claimed “thumbprint” because a thumb is a “finger” and a thumb has a fingerprint. It was known and common in the art to analyze a user’s fingerprint from their thumb as this digit is typically facing a mobile device’s touchscreen or fingerprint reader while holding the mobile device with one hand. *See* Ex-1027 ¶14 (disclosing that “references to the fingers of a user include the thumbs and that similarly a fingerprint is understood to refer to either a fingerprint or thumbprint”). This understanding 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.

165. To the extent *Grigg*'s fingerprint does not disclose a "thumbprint," *Grigg* renders this obvious. 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."); Ex-1027 ¶14. A POSITA would have modified *Grigg* to capture a "thumbprint," to the extent *Grigg* does not disclose this expressly, to capture any digits of a user and provide more options for a user requiring a fingerprint scan. This includes the thumb, which most smartphones (like those in *Grigg*) are designed to capture for fingerprint scanning. *See* Ex-1023, Fig. 11; Ex-1024, 1. This would have been nothing more than combining known elements in the prior art with understood and predictable results.

166. *Grigg* discloses, or alternatively as 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. *See* Elements [1b], [1d]. The user would provide a fingerprint via their thumb through 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 before allowing the transaction at the point-of-sale location. *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.

167. In my opinion, *Grigg* therefore discloses or at least renders obvious claim 5.

6. Claim 6

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

168. In my opinion, *Grigg* discloses a system for securely accessing a local application on a mobile device.

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

170. *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), 4:48-52 (“mobile transaction device security system 100”), 6:14-17 (“financial transaction security system”), 10:58-61 (same), 12:35-15:42 (same), 15:44-18:50 (same). *Grigg*’s discloses that its figures depict

operations of the “financial transaction security system.” *Grigg*, 3:54-67. 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.

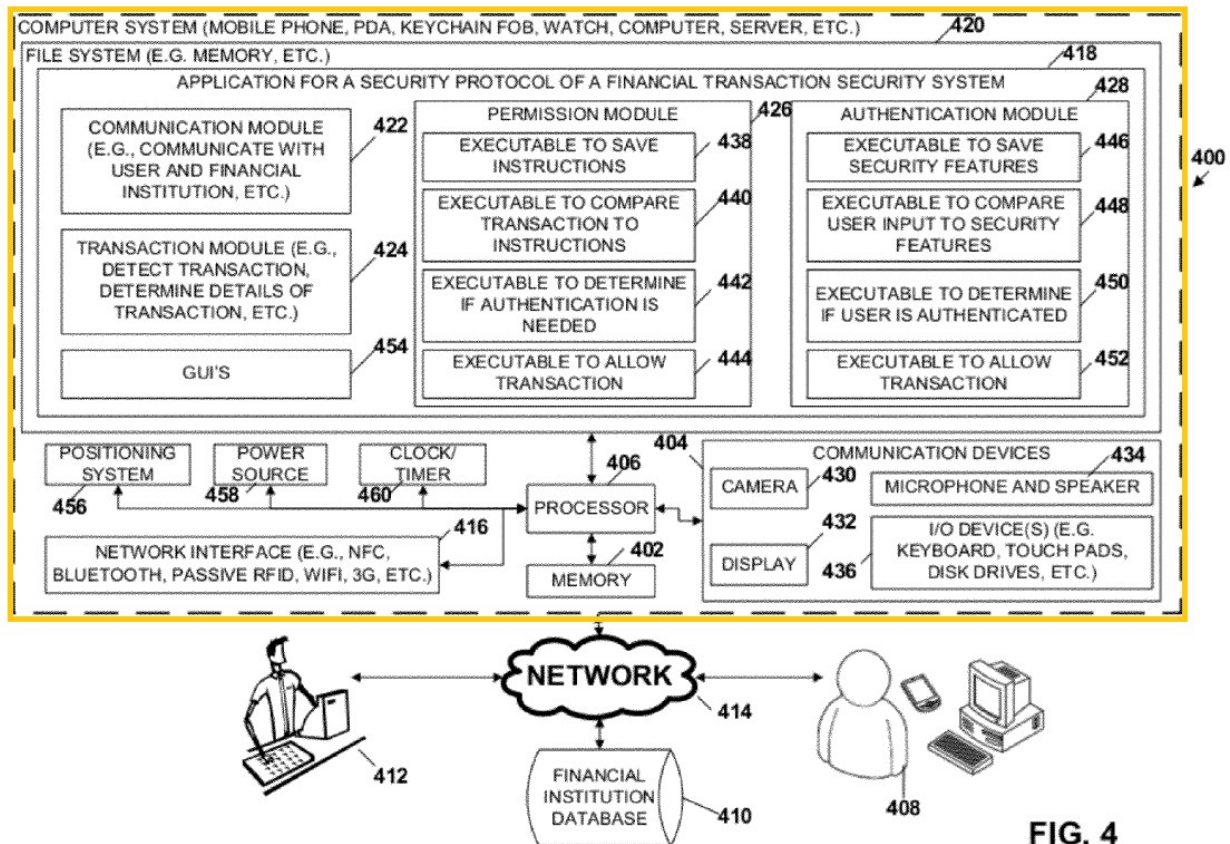


FIG. 4

Grigg, Fig. 4 (annotating system 400); 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.”).

171. In my opinion, *Grigg*'s financial transaction security system, implemented for example as a mobile phone, smartphone, PDA or the like, is the "system," as claimed.

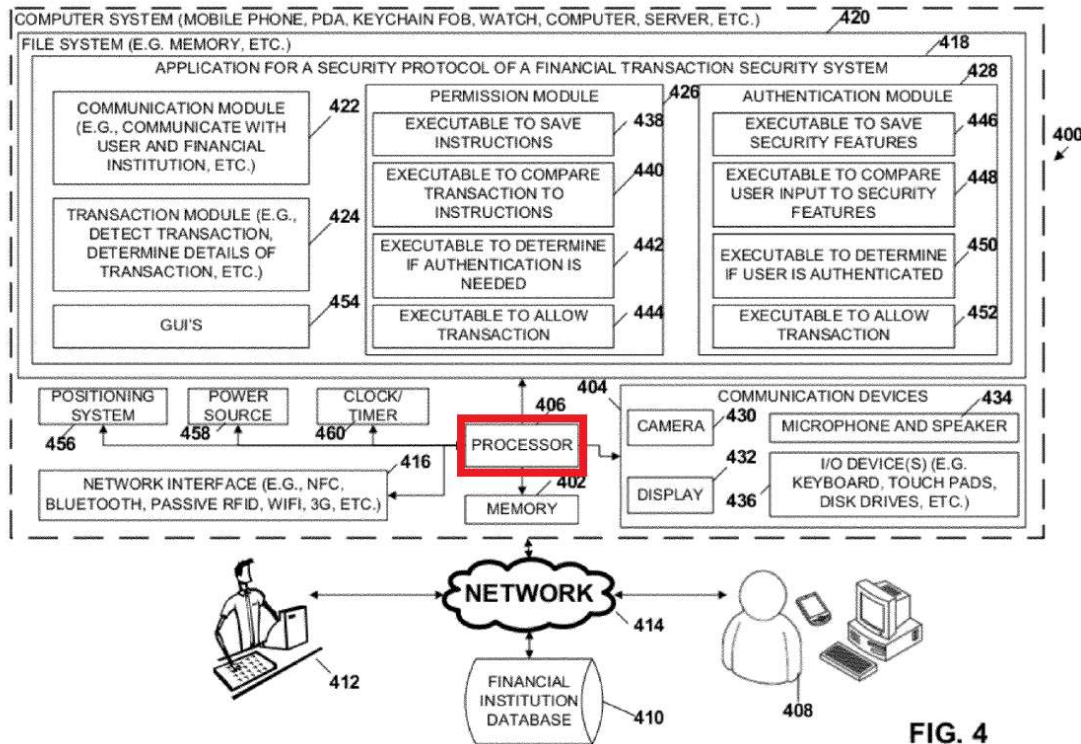
b. [6a]: "a hardware processor on a mobile device; and;"

172. In my opinion, *Grigg* discloses a hardware processor on the mobile device.

173. In my opinion, *Grigg*'s mobile device includes a hardware processor. For example, *Grigg* discloses that its financial transaction security system 400 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, 12:57-13:10, Fig. 4 (illustrating "processor 406").

174. Processing device 406 is a "hardware processor" because *Grigg* discloses it as computer hardware that may execute one or more software programs, as processors do. *Grigg*, 12:57-13:10. This may include "circuitry" or "a digital signal processor device, a microprocessor device, and various analog-to-digital converters, digital-to-analog converters, and other support circuits and/or combinations of the foregoing." *Grigg*, 12:57-13:10. *Grigg*'s system may also "take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.), or an embodiment

combining software and hardware aspects that may generally be referred to herein as a ‘system.’” *Grigg*, 18:51-67. Processing device 406 is therefore a hardware processor.



Grigg, Fig. 4 (annotating **processor 406**).

175. *Grigg* thus discloses a hardware processor on the mobile device.

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

176. 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.

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

- 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,”

178. 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].

179. *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 (GUIs) 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 *GUIs* 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.

180. 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]. *Grigg* provides exemplary depictions of this interface in Figure 9. *Grigg*, 17:49-18:50, Fig. 9.

181. *Grigg* therefore discloses and/or renders obvious Element [6c].

- 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.”**

182. 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].

183. For the reasons explained in Element [6c], *Grigg* discloses multiple interfaces or GUIs, including those for receiving security features and those for authenticating a user during a transaction. *See* Element [6b]; *Grigg*, 2:50-64 (describing an interface that allows a user to “provide[] security features ... which are then available to the mobile device” and then the user “provides input to authenticate his identity in order to allow the transaction”), 15:15-23 (describing additional interfaces, including “*GUI’s*” and “[*m*]ultiple *GUI’s*” to “assist the user in utilizing ... any other feature of the financial transaction security system 400”), 17:49-18:50 (disclosing, among others, interface 900). *Grigg* additionally 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 (e.g., for “prompt[ing] on a display screen” for input) discloses a “second interface,” as claimed.

184. *Grigg* therefore discloses or at least renders obvious Element [6d].

7. Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”

185. In my opinion, *Grigg* and modified *Grigg* discloses the additional limitation in claim 7 for the same reasons discussed for claim 2.

8. Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”

186. In my opinion, *Grigg* discloses or at least renders obvious the additional limitation in claim 8 for the same reasons discussed for claim 3.

9. Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”

187. In my opinion, *Grigg* discloses or at least renders obvious the additional limitation in claim 9 for the same reasons discussed for claim 4.

10. Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”

188. In my opinion, *Grigg* discloses or at least renders obvious the additional limitation in claim 10 for the same reasons discussed for claim 5.

B. Ground 2: *Grigg* in view of *Carter* Renders Obvious Claims 1-10

1. Motivation to Combine *Grigg* and *Carter*

189. In my opinion, 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.

190. As discussed, *Grigg* discloses a mobile device that allows a user to configure authentication of the user based on a user preference and based on a transaction amount. *See, e.g., Grigg*, 1:48-3:41, 21:58-62 (claim 13). *Carter* discloses authenticating a user in a transaction and, like *Grigg*, discloses a mobile device “configured for multi-factor authentication for transactions,” and authenticating the user using different “levels” of authentication that are cumulative of one another. *See, e.g., Carter* ¶¶31-32.

191. In my opinion, a POSITA first would have understood *Grigg* and *Carter* to be compatible. 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* ¶¶8, 47, 68. *Grigg* and *Carter* disclose similar mobile devices, including a mobile phone, smartphone, or PDA. *Grigg*, 3:15-22, 12:35-40; *Carter* ¶20. Both also focus on protecting a user’s sensitive information. *Grigg*, 1:57-60, 2:4-7 (defining a “security protocol for performing a transaction”); *Carter* ¶¶31-32 (requiring higher authentication levels to reduce “the risk of fraud”), ¶104 (“the authentication features permit secure transactions with extensive protection against fraud and identity theft”). *Grigg* and *Carter* further contemplate security “levels” for authenticating a user. *Grigg*, 7:55-60 (disclosing that “the user sets different levels of security required in different categories”), 8:35-41 (“the user is able to customize the security levels”), 14:63-15:4; *Carter* ¶¶6, 31-40. Given the overlap of *Grigg* and

Carter, in addition to the similar problems they address, a POSITA would have understood they were compatible.

192. *Carter* is also analogous art to the '347 patent because they are from the same field of endeavor: application security to protect a user's sensitive information. Like the '347 patent, *Carter* improves the security of applications by providing levels of authentication during a transaction. *Carter*, ¶¶6, 31-40. 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.

193. 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 and thus improve *Grigg*'s system. Doing so would have enabled a user to choose single or multiple levels of user authentication based on, for example, a user preference for greater security or the details of the transaction. Indeed, *Carter* expressly discloses different authentication "levels" to secure a transaction, just like *Grigg*, and expressly contemplates "cumulative" levels. *Carter* ¶¶31-32; *Grigg*, 6:37-61.

194. In my opinion, 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* ¶3. *Carter*

discloses requiring “greater authentication ... for higher value (and higher risk) purchases,” which “greatly decrease[s]” the risk of fraud. *Carter* ¶32. This includes “requir[ing] different types of authentication.” *Carter* ¶32. 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. 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* ¶¶32-39.

195. In my opinion, 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* ¶¶32-40. POSITAs also understood that multi-factor authentication was known and understood in the art, *see* Ex-1015, 3; Ex-1016, 2:21-24; Ex-1017, 1:54-64; Ex-1018, Abstract, 344-349; Ex-1019, 1, and *Carter* expressly discloses its use in the same context as *Grigg*: in a financial transaction at a point-of-sale location, *Carter* ¶¶8, 26. 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. Ex-1015, 3 (“Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods”); Ex-1017, 1:54-64 (“Even two factor authentication can virtually eliminate fraudulent transactions”). For example, it is more difficult to fraudulently conduct a transaction when multiple factors are required. Ex-1015, 3; Ex-1017, 1:54-64. 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.). In other situations, the user would be able to set the system to require only one factor.

196. 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. 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. 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). Only after a user is authenticated by the one or more authentication methods would a transaction be allowed. 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 for use in point-of-sale transactions, and POSITAs understood how to implement user interfaces to enable such functionality. *See, e.g.*, Ex-1028, 60-62.

2. Claim 1

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

197. In my opinion, *Grigg* discloses Element [1pre] for the same reasons discussed in Grounds 1A and 1B, Element [1pre].

- b. [1a]: “launching a local application on a mobile device;”**

198. In my opinion, *Grigg* discloses Element [1a] for the same reasons discussed in Grounds 1A and 1B , Element [1a].

- 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;”**

199. In my opinion, *Grigg* in view of *Carter* renders this feature obvious.

200. 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.

201. *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.

202. For example, *Carter* discloses “receiv[ing] information related to the person that can be used for authentication purposes,” including biometric information, and “authentica[t]ing the person by verifying the information received.” *Carter* ¶5. *Carter* discloses optionally requiring “higher levels or **multiple types** of authentication.” *Carter* ¶6. 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* ¶6. *Carter* thus discloses a desired security level configuration setting in its authentication levels.

203. *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* ¶¶32, 40. This may include “transaction controls” specifying the level of authentication required for a transaction. *Carter* ¶¶68-69, 40 (“the level of authentication ... may be at least partially controlled by personal preferences”), 32 (“the necessary level and type of authentication for various transactions may be controlled, at least in part, by the

person's preferences"); *see also Carter* ¶31 ("A hierarchy of authentication levels and/or authentication methods may be utilized, where a necessary authentication level and/or method is determined by characteristics or context of the transaction. Such characteristics can include the value of the transaction, the location of the transaction, [or] safety and health concerns.").

204. *Carter* discloses various authentication methods for its different levels. For example, *Carter*'s device 101 "is configured for multi-factor authentication of transactions" and that "multi-factor authentication allows for increased authentication requirements as the value of the transaction increases." *Carter* ¶¶31-32. *Carter* discloses various embodiments, including a first level requiring fingerprint authentication, a second level requiring a personal identification number (PIN), a third level requiring voice biometric identification, a fourth level requiring facial recognition, and a fifth level requiring GPS location authentication. *Carter* ¶¶33-39. According to *Carter*, the number of levels, the type of authentication for each level, and their order "may be variable and context-specific." *Carter* ¶40; *see also Carter* ¶36 (discloses voice authentication as the first level instead of fingerprint), ¶32 ("the number, type, and gradation (if any) of authentication can be varied as desired, based on the context of the transaction").

205. For its different levels, *Carter* discloses that "each increasing level of authentication may cumulatively require authentication by all of the methods of each

lower level in the hierarchy.” *Carter* ¶32; *see also Carter* at cl. 14 (“wherein each authentication level in the hierarchy of authentication levels requires an authentication method comprising the cumulative authentication methods of all lower authentication levels in the hierarchy and an additional authentication method”), ¶6 (same). Like *Grigg*, *Carter* discloses exemplary authentication methods may include “fingerprint validation, voice validation, facial recognition validation, iris scan validation, PIN validation, and GPS location validation.” *Carter* ¶7.

206. To enable its authentication, *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* ¶31. I/O 109 “may include a biometric sensor, which can collect one or more types of biometric data.” *Carter* ¶31.

207. *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. 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* ¶¶3-6, 31-40. Each of *Carter*’s security levels corresponds to a different security level scan (i.e., authentication method(s)). *See Carter* ¶69,

claim 9 (“wherein each authentication level requires a different authentication method”). *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* ¶32 (“[T]he necessary level and type of authentication for various transactions may be controlled, at least in part, by the person’s preferences,” and “the person may have at least some control over the specific values where the authentication level changes.”); *see also Carter* ¶¶ 28, 40.

208. In my opinion, in the combined *Grigg-Carter* device, a POSITA would have set a desired authentication level based on user preferences, which would have required one or more of *Carter*’s authentication methods before enabling the device to perform a transaction. 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. *See Carter* ¶69 (determining authentication level “based on factors such as value and type of transactions”); *see also Carter* ¶40 (contemplating “levels of authentication” being “dependent on the value of the transaction”). For example, below \$100 a user only needs to input a password. For transactions above \$100, the user needs to authenticate herself using multiple, cumulative security levels, including a password and biometric information. 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.

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

209. In my opinion, *Grigg* discloses Element [1c] for the same reasons discussed in Grounds 1A and 1B, Element [1c].

- 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.”**

210. In my opinion, *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].

211. 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.

212. 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* ¶68. “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* ¶69. *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* ¶32. This includes, for example, “the person may hav[ing] at least some control over the specific values where the authentication level changes.” *Carter* ¶32; *see also Carter* ¶¶68-69 (referencing “pre-set purchasing preferences”), claim 15 (“wherein the necessary authentication level for the transaction is determined based on preferences previously indicated by the person”). In some embodiments, user preferences or different transaction amounts can trigger different levels of authentication. *Carter* ¶¶33-40, 69.

213. In the combined *Grigg-Carter* system, a user would set the desired level of authentication based on a user preference or alternatively based on a dollar amount of 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. Element [1c] (Grounds 1A, 1B); *Grigg*, 5:12-31, 9:32-42, 13:36-44; *Carter* ¶¶68 (“the person (customer) initiates the transaction”).

214. In the combined system, 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. *Carter* ¶¶32. For example, based on the user preference, one authentication method or multiple cumulative methods are required before allowing a transaction to proceed. 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. *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. *Carter* ¶¶6, 32, cl. 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*”).

215. In my opinion, *Grigg* in view of *Carter* therefore renders Element [1d] obvious.

3. Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”

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

4. Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”

217. In my opinion, 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. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the “plurality of security level scans.” *Carter* ¶¶31, 33-39; *see also* Element [1b], Ground 2.

5. Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”

218. In my opinion, in *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 4 for the same reasons discussed for claim 4, Grounds 1A and 1B. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the “plurality of security level scans.” *Carter* ¶¶31, 33-39.

6. Claim 5: “The method of claim 3, wherein the biometric scan includes a thumbprint.”

219. In my opinion, in *Grigg-Carter*, *Grigg* discloses the additional limitation in claim 5 for the same reasons discussed for claim 5, Grounds 1A and 1B. *Carter* also discloses this feature in addition to rendering obvious a biometric scan being one of the “plurality of security level scans.” *Carter* ¶¶31, 33-39.

7. **Claim 6**

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

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

- b. **[6a]: “a hardware processor on a mobile device; and a local application on the mobile device and configured to be executed by the hardware processor;”**

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

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

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

- 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,”**

223. In my opinion, in *Grigg-Carter*, *Grigg* discloses the “first interface” in Element [6c] for the same reasons discussed for Element [6c], Grounds 1A and 1B.

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

- 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.”**

225. In my opinion, in *Grigg-Carter*, *Grigg* discloses the “second interface” in Element [6d] for the same reasons discussed for Element [6d], Grounds 1A and 1B.

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

8. Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”

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

9. Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”

228. In my opinion, 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. *Carter* also discloses this feature, in addition to rendering obvious a biometric scan being one of the “plurality of security level scans.” *Carter* ¶¶31, 33-39; *see also* Element [1b], Ground 2.

10. Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”

229. In my opinion, 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. *Carter* also discloses this feature. *Carter* ¶¶31, 33-39.

11. Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”

230. In my opinion, 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. *Carter* also discloses this feature. *Carter* ¶¶31, 33-39.

C. Grounds 3A and 3B: *Google* Anticipates and/or Renders Obvious Claims 1, 2, 6, and 7

1. Claim 1

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

231. In my opinion, *Google* discloses a method of securely accessing a Google Account, including Google’s mailbox provider, Gmail. *Google*, 1.

232. A POSITA would have understood that Gmail was accessible from a web browser (“a local application”) on a mobile device. 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”). 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.

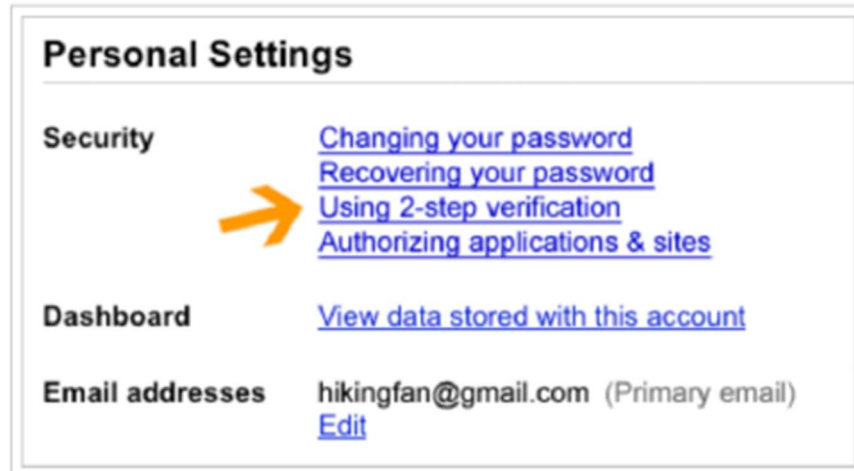
233. To further strengthen the security offered by a single password, *Google* discloses “an advanced opt-in security feature called 2-step verification that makes your Google Account [(including, e.g., Gmail)] significantly more secure by helping to verify ... the real owner of your account.” *Google*, 1. 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. Thus, *Google* discloses the preamble.

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

234. In my opinion, *Google* discloses [1a]. 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. 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.

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;”

235. In my opinion, *Google* discloses and/or renders obvious [1b]. 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.

236. 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”). *Google*, 1. *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.” *Google*, 1.

237. In my opinion, a POSITA would have understood that an “opt-in” feature requires a user to specifically turn on that feature to enable it. 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”).

238. 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"). 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").

239. In my opinion, 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. 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. In addition to improving user experience, including this functionality in the mobile application itself would advantageously encourage adoption of 2-step authentication. 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.

240. In my opinion, 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. 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.

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

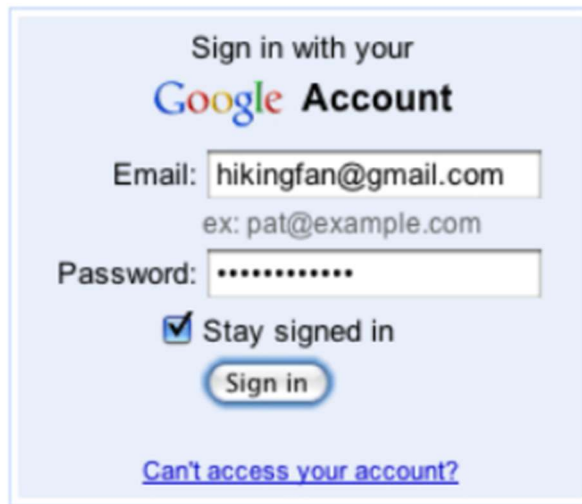
241. In my opinion, *Google* discloses [1c]. As discussed for [1pre] and [1a], Gmail may be accessed through a web browser (“local application”) or mobile application (“local application”). *See* Elements [1pre], [1a]. A POSITA would have understood that, once the security configuration has been established 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.

- 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.”**

242. In my opinion, *Google* discloses [1d]. 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.

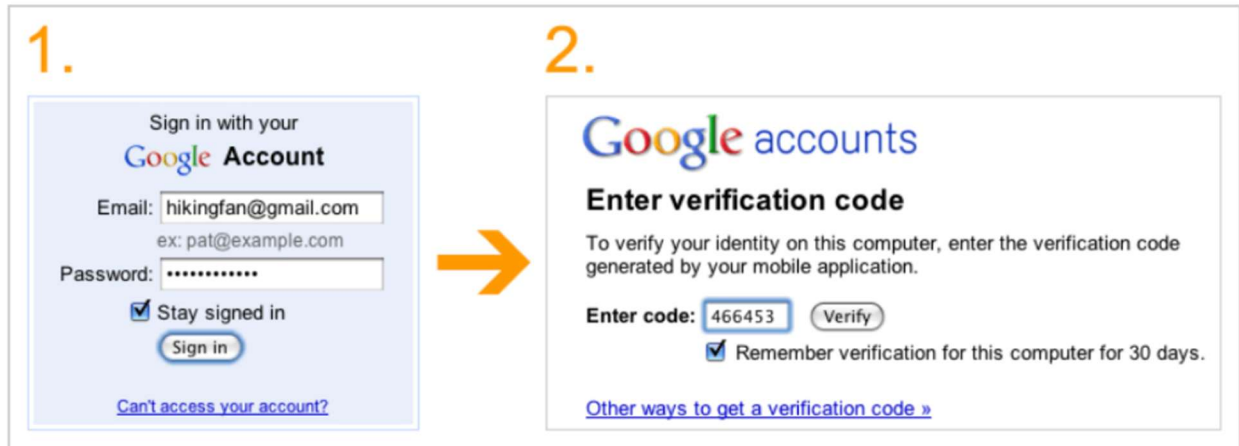
243. Where a user has declined to opt into 2-factor authentication (“when the desired security level configuration setting is set to a single security level”), the authentication process will only request a password (“the authentication process including only a single security level scan”). *Google*,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

1.



Google, 1 (cropped).

244. 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.” *Google*, 1.



Google, 1.

245. “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.” *Google*, 1. Once this code has been entered, the user can access their Google Account, including Gmail.

2. Claim 2: “The method of claim 1, wherein the single security level scan includes a request for a password.”

246. In my opinion, *Google* discloses the additional limitation in claim 2. As discussed above, *Google*’s single security level scan includes a request for a password. *Google*, 1.

3. Claim 6

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

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

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

248. In my opinion, *Google* discloses or at least renders obvious [6a]. 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 include a “hardware processor.” Ex-1025, 1 (iPhone 4 “released 2010, June” having “1.0 GHz Cortex-AB” CPU).”

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

249. In my opinion, *Google* discloses or at least renders obvious [6b]. 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. 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. This is how mobile phones operate.

- 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,”**

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

- 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.”**

251. In my opinion, *Google* discloses claim [6d] for the same reasons discussed for Element [1d], Grounds 3A and 3B.

- 4. **Claim 7: “The system of claim 6, wherein the single security level scan includes a request for a password.”**

252. In my opinion, *Google* discloses the additional limitation in claim 7 for the same reasons discussed for claim 2.

D. Ground 4: *Google* in view of *Carter* Renders Obvious Claims 3-5 and 8-10

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

253. In my opinion, it would have been obvious to a POSITA to improve *Google*'s 2-factor authentication by including *Carter*'s biometric authentication.

254. 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.

255. In my opinion, a POSITA would have understood that biometric-based access control can be based on different elements of a person’s body, each with their own benefits. 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* ¶7.

256. A POSITA would have understood the benefits associated with using fingerprint scanning, including scanning a thumbprint. According to *Carter*, “fingerprint authentication can be required for all transactions, due to its ease and simplicity.” *Carter* ¶34. A POSITA would have understood that *Carter*’s statement applied equally to a thumbprint. *See* Grounds 1A and 1B, claim 5; *see* Ex-1023, 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. To the extent *Carter*’s fingerprint does not disclose a “thumbprint,” *Carter* renders this obvious. *See* Ground 4, claim 5.

257. A POSITA would have also understood the benefits associated with using voice validation. 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.

258. In my opinion, 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. *Carter* teaches that a “mobile device may contain a biometric sensor to read biometric information.” *Carter* ¶8. *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* ¶31. 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. This includes the functionality of the iPhone available as of the critical date. Ex-1025, 1-2.

2. Claim 3: “The method of claim 1, wherein the plurality of security level scans includes a biometric scan.”

259. In my opinion, the *Google-Carter* combination renders obvious claim 3. As discussed in above in the reasons for combining *Google* and *Carter*, 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. *Carter* teaches the use of a variety of biometric scans, including “fingerprint validation, voice validation, facial recognition validation, [and] iris scan validation.” *Carter* ¶7.

3. Claim 4: “The method of claim 3, wherein the biometric scan includes a voiceprint.”

260. In my opinion, the *Google-Carter* combination renders obvious claim 4. As discussed in above in the reasons for combining *Google* and *Carter*, 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 the reasons for combining *Google* and *Carter*, 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* ¶7.

4. Claim 5: "The method of claim 3, wherein the biometric scan includes a thumbprint."

261. In my opinion, the *Google-Carter* combination renders obvious claim 5. As discussed in above in the reasons for combining *Google* and *Carter*, 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 the reasons for combining *Google* and *Carter*, 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* ¶7.

262. To the extent *Carter*'s fingerprint does not disclose a "thumbprint," *Carter* renders this obvious. 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."). 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. This includes the thumb, which most

smartphones (like those in *Carter* and *Google*) are designed to capture for fingerprint scanning. See Ex-1023, Fig. 11; Ex-1024, 1. This would have been nothing more than combining known elements in the prior art with understood and predictable results.

5. Claim 8: “The system of claim 6, wherein the plurality of security level scans includes a biometric scan.”

263. In my opinion, the *Google-Carter* combination renders obvious the additional limitation in claim 8 for the same reasons discussed for claim 3, Ground 4.

6. Claim 9: “The system of claim 8, wherein the biometric scan includes a voiceprint.”

264. In my opinion, the *Google-Carter* combination renders obvious the additional limitation in claim 9 for the same reasons discussed for claim 4, Ground 4.

7. Claim 10: “The system of claim 8, wherein the biometric scan includes a thumbprint.”

265. In my opinion, the *Google-Carter* combination renders obvious the additional limitation in claim 10 for the same reasons discussed for claim 5, Ground 4.

X. CONCLUSION

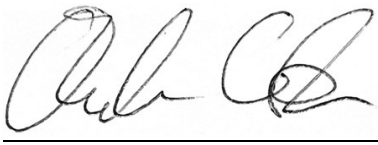
266. For the reasons set forth above, it is my opinion that claims 1-10 of the '347 patent are unpatentable in view of the prior art.

267. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the

United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination may take place within the United States. If cross-examination is required of me, I will appear for cross-examination during the time allotted for cross-examination.

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

Dated: 1st October, 2025

By: 

Andrew Cockburn, Ph.D.