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
U.S. Patent No. 12,014,347

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PATENT OWNER'S EXHIBIT LIST

EXHIBIT	DESCRIPTION
2001	Excerpts of File History for U.S. Patent Application Publication No. 2015/0161592
2002	Complaint for Patent Infringement, *PayGeo, LLC v. Samsung Elecs. Co.*, No. 25-cv-00334-RWS-RSP, Dkt. No. 1 (E.D. Tex. Apr. 2, 2025)
2003	Second Amended Docket Control Order, *PayGeo, LLC v. Samsung Elecs. Co.*, No. 25-cv-00334-RWS-RSP, Dkt. No. 52 (E.D. Tex. Oct. 2, 2025)
2004	Order, *Resonant Sys., Inc. v. Sony Grp. Corp.*, No. 2:22-cv-00424-JRG, Dkt. No. 84 (E.D. Tex. July 9, 2024)
2005	Excerpts of Defendants' Invalidity Contentions, *PayGeo, LLC v. Samsung Elecs. Co.*, No. 25-cv-00334-RWS-RSP (E.D. Tex.), served on November 3, 2025
2006	Docket Navigator webpage, Motion Outcomes for Motions to Stay Pending *Inter Partes* Review in the Eastern District of Texas, dated January 1, 2020 through November 21, 2025
2007	Lex Machina webpage, Motion Metrics for Stay Pending PTAB in the Eastern District of Texas, dated January 1, 2020 through November 21, 2025
2008	Excerpts from U.S. District Court – Federal Case Management Statistics, Median Time from Filings to Trial (E.D. Tex.), 12-Month Periods Ending June 30, 2025, available at https://www.uscourts.gov/sites/default/files/document/fcms_na_distprofile0630.2025.pdf
2009	Docket Navigator webpage, Time to Trial in the Eastern District of Texas, dated January 1, 2022 through November 21, 2025
2010	U.S. Patent Application Publication No. 2013/0024360-A1

EXHIBIT	DESCRIPTION
2011	Order, *Kirsch Rsch. and Dev. LLC v. DuPont de Nemours, Inc.*, No. 5:20-cv-00057-RWS, Dkt. No. 269 (E.D. Tex. July 7, 2021)

I. INTRODUCTION

The Director should deny institution because the asserted references do not disclose defining a "desired security level configuration setting" in a local application of a mobile device and that "establish[es] 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." Ex. 1001 (U.S. Patent No. 12,014,347, or "the '347 Patent") at 24:23-29, 24:32-41.

Grigg (Grounds 1 and 2) does not disclose establishing whether the local application requires a single security level or a plurality of security levels before allowing access to a feature of the local application. In contrast, *Grigg* disclosed techniques for reducing protections on the basis that onerous authentication processes bog down financial transactions and waste the time and effort of those conducting transactions. In *Grigg's* system, the user is permitted to allow some transactions with no authentication whatsoever, so *Grigg* does not disclose "requiring . . . the user to perform an authentication process" before "allowing access to the at least one feature of the local application." '347 Patent, limitation [1d].

Grigg also does not anticipate the claims because it does not disclose a configuration setting that can specify requiring "a plurality of security levels before allowing access to at least a feature in the local application." *Id.*, limitation [1b]. *Grigg* allows, at most, a single security level for transactions exceeding some specified threshold value. Samsung has also not established that it would have been obvious to modify *Grigg* (Grounds 1B and 2) to satisfy this limitation. Indeed, Samsung's proposed modifications would vitiate *Grigg*'s stated objective, which is to reduce inconveniences to the user due to onerous authentication procedures.

Samsung's challenges based on a Google blog article (Grounds 3A, 3B, and 4) are similarly without merit. Samsung's argument for anticipation in view of the Google blog article is fundamentally flawed because it improperly relies on a combination of extrinsic evidence outside the four corners of the Google blog article to fill in missing claim limitations, including "a local application on a mobile device." Even if that combination of evidence were permissible, Samsung's mapping of the "local application" to either a mobile web browser or a standalone Gmail application fails to satisfy the requirements of the Challenged Claims. A POSITA would not understand the Gmail web service to be a feature of a mobile web browser, and therefore does not disclose "before allowing access to the least ***one feature of the local application***." Finally, a standalone Gmail application fails to disclose "enabling a user to set a desired security level configuration setting ***in the local application for the mobile device***" because the alleged "desired security level configuration settings" are not set in the standalone Gmail application, but in a webpage for Google Account Settings.

Thus, Petitioner Samsung has failed to show that there is a reasonable likelihood that they would prevail with respect to at least one Challenged Claim, and institution should be denied.

II. OVERVIEW

A. The '347 Patent

Independent Claims 1 and 6 recite methods and systems for securely accessing a local application on a mobile device. '347 Patent at 24:20-21, 24:50-51. The method includes launching a local application on a mobile device and enabling a user to set a desired security level configuration setting in the local application for the mobile device. *Id.* at 24:23-25; 10:32-53. The desired security level configuration setting 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. *Id.* at 24:25-29, 11:62-12:13. Upon launching the local application, the system requires the user to perform the chosen authentication process before allowing access to the at least one feature of the local application. *Id.* at 24:25-41, 11:26-41.

B. Overview of *Grigg* (Ex. 1005)

Grigg (U.S. Patent No. 8,195,576) discloses a "mobile transaction device security system" for improving a "mobile wallet" for engaging in financial transactions. *Grigg* at 1 (field 54), 1:25-41. In a typical "mobile wallet," the user's mobile phone communicates payment information to a point-of sale (POS) terminal, and the POS terminal uses the payment information to approve the transaction. *Id*. at 1:25-41. Mobile wallet systems also required onerous steps to verify the user's identity, which according to *Grigg* are "inconveniences" that "can add up to wasted time, effort, and worry for people as they conduct transactions." *Id*.

In an attempt to cure these identified deficiencies with mobile wallets of the time, *Grigg* teaches "allowing transactions without authentication." *Grigg* at Abstract. *Grigg*'s user "provides instructions relating to when the user does not need to authenticate his identity to perform a transaction." *Id.* at 2:21-23, 5:2-5, 5:34-57. "For example, the user may not require authentication for transactions of less than five dollars. In some embodiments, the instructions relate to the financial account of the user, such as the balance in the financial account or previous purchases by the user from the account." *Id.* at 2:27-31.

Because *Grigg* teaches a system that allows financial transactions without requiring the user to authenticate first, *Grigg* fails to disclose "requiring . . . the user to perform an authentication process" (whether "only a single security level scan" or a "plurality of security level scans") "***before allowing access*** to the at least one feature of the local application." '347 Patent at 24:32-41 (Claim 1) (emphasis added), 24:61-25:5 (Claim 6). *Grigg* also does not disclose "enabling a user to set a desired security level configuration setting in the local application for the mobile device" where "the desired security level configuration setting establish[es] 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." '347 Pat at 24:23-29 (Claim 1), 24:54-61 (Claim 6).

C. Overview of the *Google* blog article (Ex. 1007)

The Google blog article is an archived blog post from the "Official Google Blog," describing the release of a security feature called "2-step verification" for a user's Google Account. *Google* at 1. The single-page Google blog article provides few details, and makes no mention of a mobile web browser or a standalone Gmail application. The Google blog article fails to disclose "launching ***a local application*** on a mobile device" and fails to meet the claimed requirements of "enabling a user to set a desired security level configuration setting ***in the local application*** for the mobile device," or "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." '347 Patent, Claim 1 (emphasis added); Claim 6 (similar).

D. Overview of *Carter* (Ex. 1006)

Carter is U.S. Patent Application Publication No. 2009/0152343 A1, entitled "Authentication methods for use in financial transactions and information banking." *Carter* at Cover, (54). *Carter* discuses "[a] necessary authentication level for the transaction can be designated from among the hierarchy, and each level of the hierarchy may require the cumulative authentication methods of one or more of the lower levels in the hierarchy." *Id.* at [0006].

Carter is relied upon in obviousness Ground 2 as a backup reference to redundantly argue that the asserted references render obvious limitations [1b] and [1d]. Pet. at 57-63. *Carter* is also relied upon in obviousness Ground 4 to argue that dependent claims 3-5 and 8-10 are rendered obvious by Google in view of *Carter*. *Id*. at 79-83. *Carter* fails to teach a modification to either *Grigg* or the Google blog article that would yield "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." '347 Patent at 24:25-29, 24:57-61.

III. SAMSUNG'S PROPOSED UNPATENTABILITY GROUNDS

The Petition presents the following grounds for challenging the claims of the '347 Patent.

Ground	Claims	Basis	References Relied Upon
1A	1-10	§ 102	*Grigg* (Ex. 1005)
1B	1-10	§ 103	*Grigg* (Ex. 1005)
2	1-10	§ 103	*Grigg* (Ex. 1005) and *Carter* (Ex. 1006)
3A	1, 2, 6, 7	§ 102	*Google* (Ex. 1007)

3B	1, 2, 6, 7	§ 103	*Google* (Ex. 1007)
4	3-5, 8-10	§ 103	*Google* (Ex. 1007) and *Carter* (Ex. 1006)

Pet. at 9.

Although there are multiple reasons the '347 Patent is valid over *Grigg*, *Carter*, and *Google*, this Preliminary Response focuses on only limited reasons why post grant review should not be instituted. *See Travelocity.com L.P. v. Cronos Techs., LLC*, No. CBM2014-00082, Paper 12 at 10 (P.T.A.B. Oct. 16, 2014) ("[N]othing may be gleaned from the Patent Owner's challenge or failure to challenge the grounds of unpatentability for any particular reason.").

IV. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this Preliminary Response, PayGeo adopts Samsung's definition of a person of ordinary skill in the art: "A person of ordinary skill in the art ('POSITA') would have had at least a bachelor's degree in electrical engineering, computer science, or a similar field and two years of experience designing graphical user interfaces, including those for mobile devices . . . . Additional relevant work experience can compensate for less education, and vice versa." Pet. at 7.

V. THE CHALLENGED CLAIMS ARE PATENTABLE

A. *Grigg* Does Not Anticipate the Challenged Claims (Ground 1A)

1. *Grigg* Does Not Disclose a Desired Security Level Configuration Setting Establishing Whether a Local Application Requires a Single or Plurality of Security Levels

Samsung's anticipation Ground 1A fails because *Grigg* does not disclose limitation [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." Pet. at 17-28 (emphasis added). Independent claim 6 recites a similar limitation [6c]. *Id*. at 48-49.

Grigg does not disclose 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. Instead, *Grigg* discloses a financial security system where a user can specify that authentication is not needed to perform a transaction (i.e., zero security features) or, at most, one security feature is needed to perform a transaction. *Grigg* at 3:5-10 ("[T]he user is able to provide instructions for allowing a transaction without requiring authentication of the user's identity.").

Grigg's failure to teach requiring multiple security levels before allowing access to a feature in a local application is consistent with its stated objective for improving "mobile transaction security in a way that is both convenient and effective for the interested parties." *Grigg* at 1:42-44. Specifically, *Grigg*'s Background section teaches that mobile wallet systems often require the user to take "one or more steps to authenticate the user's identity, such as the steps of having to enter a PIN, show a picture ID, provide a signature, etc." and that these multiple steps are "inconveniences [that] can add up to wasted time, effort, and worry for people as they conduct transactions." *Id.* at 1:30-36. For that reason, *Grigg* teaches reducing these "inconveniences" by reducing the number of security steps needed to approve a transaction, by specifying certain transactions do not require authentication (i.e., zero security features). *Id.*; *id.* at 3:5-10.

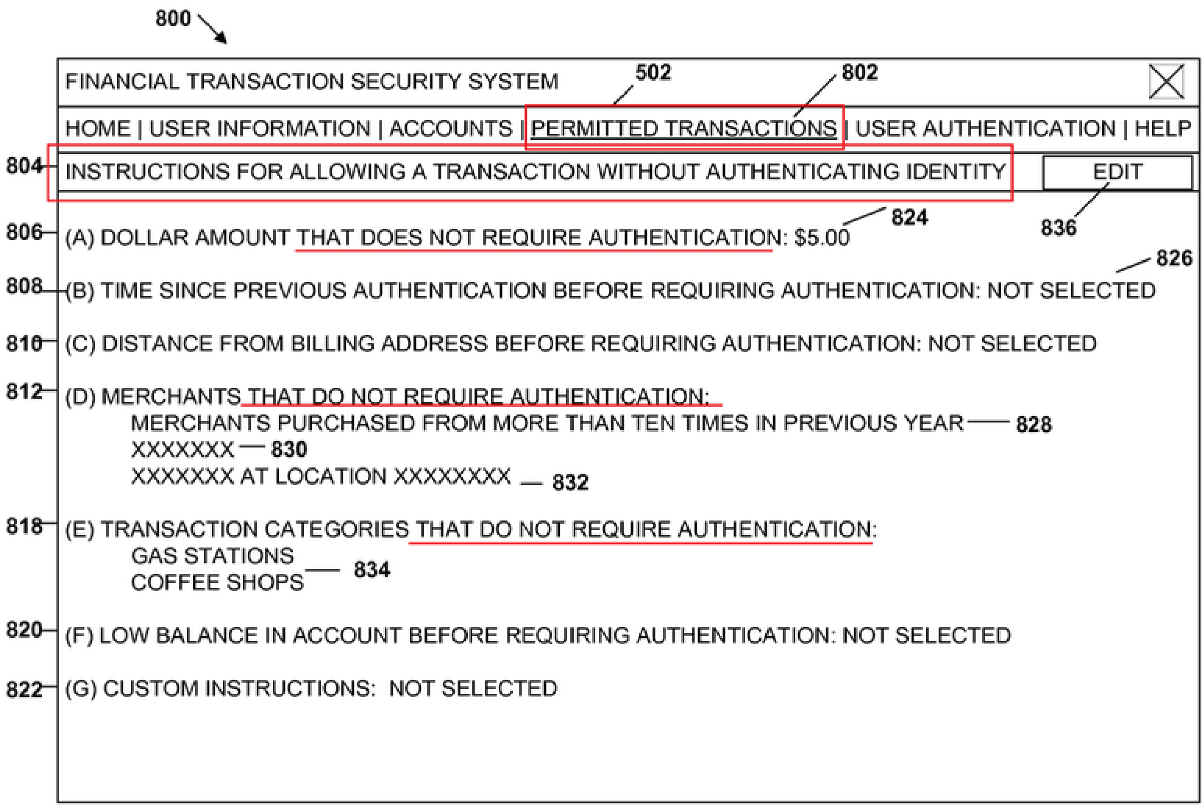


FIG. 8

Grigg at Fig. 8 (annotations added), 4:11-14 (depicting an entire graphic user interface 800 for "viewing and editing instructions for allowing a transaction without requiring authentication"), 17:48-18:16 (describing user interface 800).

Samsung cites to various instances in *Grigg* where plural nouns are used to describe *Grigg*'s authentication module "with more than one security feature," but *Grigg* does not disclose specifying an authentication process that enables the user to choose more than one security feature for any given transaction. *See* Pet. at 21 (citing *Grigg* at 6:21-23, 20:62-65, 21:58-62). Accordingly, while Samsung cites *Grigg*'s discussion of "different tiers of authentication," those "tiers" only include zero or one security feature "depending on the transaction amount." *Id.* (citing *Grigg* at 10:66-11:23); *Grigg* at 11:17-23. Thus, *Grigg* teaches no authentication at all (for transactions less than $5), a username and password (for transactions between $5 and $100), ***or*** a biometric scan (for transactions more than $100), but none of the tiers includes multiple security levels. *Grigg* at 11:17-23; *see also id.* at 6:45-61 (disclosing an example of "tiered levels," where the requirement is no authentication, user name and password, ***or*** a biometric scan, but not multiple security features).

Similarly, Samsung cites to *Grigg*'s discussion of "different levels of security," but *Grigg* teaches that these are "different levels of security for different categories," specifically either "no authentication" (i.e., zero security features) at all for gas stations while restaurants require "**a** higher level of security" (i.e., just one security feature). Pet. at 21 (*Grigg* at 7:56-60); *see also Grigg* at 8:31-41 (similar).

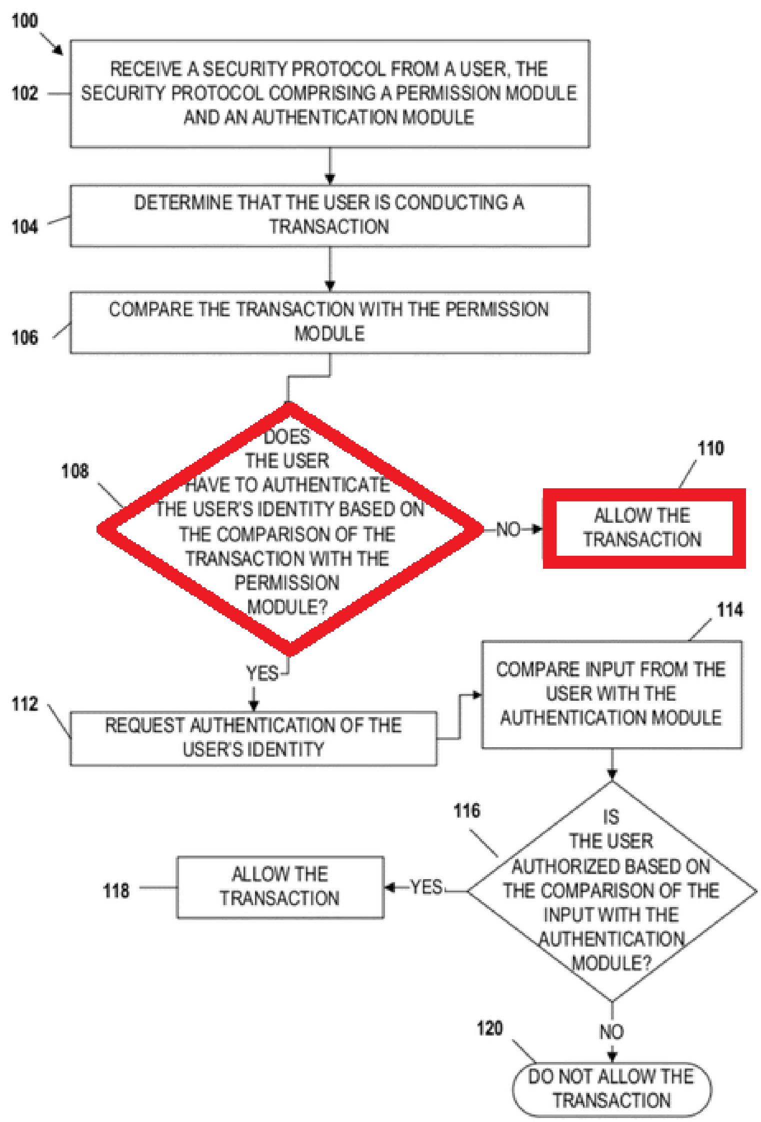
Samsung also cites to *Grigg*'s discussion of "different types of authentication" or receiving user input "of at least one" authentication method, but this is nothing more than a list of available security features for a user to choose one of. Pet. at 21-22 (citing *Grigg* at 21:58-62, 6:45-61); *see Grigg* at 15:51-52 (describing "the types of user authentication available to the user 510"). *Grigg*, therefore, fails to disclose a security level configuration setting establishing whether the local application requires ***a plurality of security levels*** before allowing access to at least a feature in the local application.

A prior art reference only anticipates a patent's claim under § 102(e) "when the four corners of [that] . . . document describe every element of the claimed invention, either expressly or inherently, such that a [POSITA] could practice the invention without undue experimentation." *Spansion, Inc. v. Int'l Trade Comm'n*, 629 F.3d 1331, 1356 (Fed. Cir. 2010) (cleaned up). Here, Samsung has failed to show that *Grigg* teaches every element of the claimed invention, including limitation [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."

2. *Grigg* Does Not Teach Requiring, Before Allowing Access to a Feature of the Local Application, the User to Perform an Authentication Process That Includes a Single Security Level Scan or a Plurality of Security Level Scans (limitation [1d])

Samsung's anticipation Ground 1A also fails because *Grigg* does not disclose limitation [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." Pet. at 31-33 (emphasis added); *see also id.* at 28. Independent claim 6 recites a similar limitation [6d]. *Id.* at 50-51.

Grigg does not disclose "requiring, before allowing access to [a] feature of the local application, the user to perform an authentication process" because *Grigg* instead teaches bypassing authentication altogether. *Grigg* at Abstract ("The security protocol includes instructions for allowing transactions without authentication . . . ."). *Grigg* teaches a security protocol having a "permission module" that "includes the instructions relating to when the user does not need to authenticate his identity as well as any hardware and/or software used to implement those instructions." *Id.* at 4:54-5:5. *Grigg* discloses "the system 100 can determine whether the user ***does not need to authenticate*** his identity before allowing a transaction" (block 108) and "if the user ***does not need to authenticate*** his identity the transaction is automatically allowed" (at block 110). *Id.* at 5:32-41 (emphasis added). In the Fig. 1 of *Grigg* annotated below, the blocks 108, 110 occur, allowing a transaction, prior to and without needing any of "authentication of the user's identity" in block 112.



Grigg, Fig. 1 (annotated). This demonstrates that *Grigg* contradicts the express limitations of the Challenged Claims, which include "requiring . . . the user to perform an authentication process" (whether "only a single security level scan" or a "plurality of security level scans") "***before allowing access*** to the at least one feature of the local application." '347 Patent at 24:32-41 (emphasis added).

Grigg repeatedly discloses removing the requirement of any authentication before allowing a transaction. For example, *Grigg* teaches not requiring authentication before allowing a transaction if the transaction amount is less than a predetermined amount (6:37-41) or if the transaction is performed within a certain distance of the user's home (6:62-7:18). *Grigg* also teaches not requiring authentication before allowing a transaction during predetermined time windows, such as "during work hours" (7:19-41), or when the transactions are "within a specific category," for example, to facilitate "quick and easy" transactions at gas stations. *Grigg* at 7:42-60. In another example, *Grigg* teaches not requiring authentication before allowing a transaction "based on the transaction merchant," including "at predetermined specific merchants." *Id.* at 7:61-8:17. *Grigg* further provides a user interface with a "permitted transaction tab 802" for providing "instructions for allowing a transaction without authenticating identity":

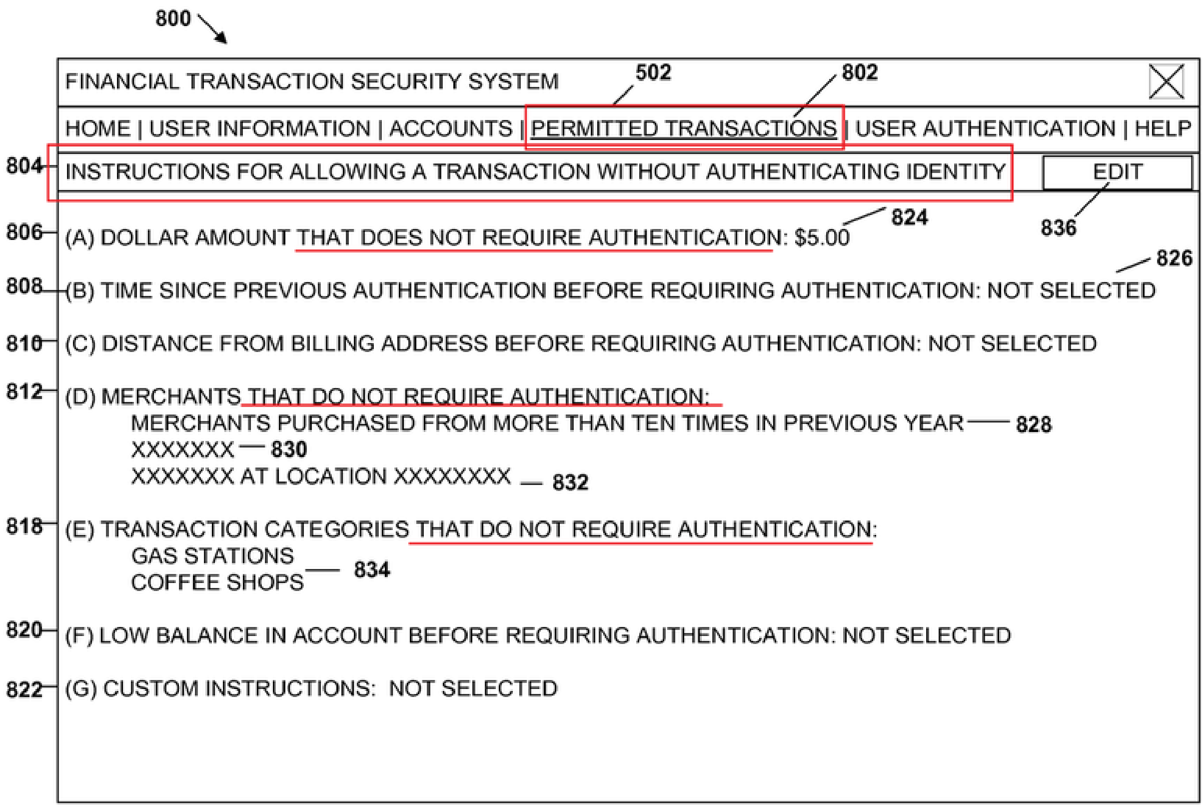


FIG. 8

Grigg, Fig. 8 (annotated) (showing instructions for transactions' dollar amount, merchants, and transaction categories that do not require authentication); *id.* at 17:49-18:16.

Accordingly, *Grigg* fails to disclose "***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," because there is no requirement to perform any authentication process in order to conduct a transaction.

B. *Grigg* Alone or With *Carter* Does Not Render Obvious the Challenged Claims (Grounds 1B and 2)

Tacitly recognizing the weakness of its anticipation grounds based on *Grigg*, Samsung provides two backup arguments for the claimed "a plurality of security levels." First, Samsung argues "[t]o the extent *Grigg* does not expressly disclose this" element, that limitation [1b] is obvious in a single-reference obviousness ground using *Grigg* (Ground 1B). Pet. at 22-28. Second, Samsung argues for a combination with the secondary reference *Carter* to satisfy "a plurality of security levels." *Id*. at 57-63. Both of these obviousness arguments fail because of a lack of motivation to combine or modify the references to yield the Challenged Claims.

There is no motivation to modify *Grigg* alone (Ground 1A) or in combination with *Carter* (Ground 2) because *Grigg* itself discourages or teaches away from using multiple or cumulative security features for a single transaction. Pet. at 23-28, 53-56. Evidence suggesting reasons to combine cannot be viewed in a vacuum apart from evidence suggesting reasons not to combine. *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1363 (Fed. Cir. 2017) ("In this case, the same reference suggests a reason to combine, but also suggests reasons that a skilled artisan would be discouraged from pursuing such a combination.").

Samsung misapprehends *Grigg*'s desire for "flexibility" as a call for multiple or cumulative authentication security steps. Pet. at 23 (citing *Grigg* at 3:10-14). This is incorrect because, as discussed above, *Grigg* identifies the drawbacks of mobile wallet systems that often require the user to take multiple "steps to authenticate the user's identity, such as the steps of having to enter a PIN, show a picture ID, provide a signature, etc." and that these multiple steps are "inconveniences [that] can add up to wasted time, effort, and worry for people as they conduct transactions." *Grigg* at 1:30-36; *see also id.* at 1:6-7 ("People desire convenience and speed when conducting financial transactions.")

For these reasons, *Grigg* discloses an entire system and user interface for settings instructions for certain types of transactions that can be approved ***without any authentication whatsoever*** (i.e., zero security authentication steps). *Grigg* at Abstract ("security protocol includes instructions for allowing transactions <u>***without authentication***</u>") (emphasis added), 20:48-50 (Claim 1 of *Grigg* claiming "allowing the transaction if the user is not required to authenticate the user's identity based on the comparison"). As such, when considering the disclosure of *Grigg* as a whole, a POSITA would not be motivated to stack multiple, inconvenient authentication security steps which would "add up to wasted time, effort, and worry." *Id.* at 1:35-41; *id.* at 7:17-18 ("The user may desire to allow transactions without authentication for convenience or security."); *id.* at 7:38-41 ("Again, by allowing customization of when the user does not need to authenticate his identity the system provides convenience along with customized security for financial transactions."). *See Arctic Cat,* 876 F.3d at 1360 (finding "it is error to fail to consider the entirety of the art" including "prior art [that] could contain one reference suggesting a combination and others critiquing or otherwise discouraging the same").

Accordingly, *Grigg*, alone or in combination with *Carter*, fails to render obvious "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."

C. The Google Blog Article, Alone or in View of *Carter*, Does Not Disclose Requiring, Before Allowing Access to a Feature of the Local Application, the User to Perform an Authentication Process (Grounds 3A-3B, 4)

The single-page Google blog article (Ex. 1007) announcing "[a]dvanced sign-in security for . . . Google account[s]" is inadequate evidence that fails to describe or render obvious every element of the Challenged Claims. *Google* at 1. Specifically, the Google blog article, alone or in combination with *Carter*, does not teach that the requisite "local application on a mobile device" was known at the time the invention was made (July 18, 2011).

Samsung presents two theories for how the Google blog article satisfies the claimed "local application on a mobile device": (1) a mobile phone web browser, and (2) a standalone Gmail application on a mobile device. Pet. at 68, 70-71. But, Samsung does not cite to any portion of the Google blog article for disclosing a mobile phone web browser or a standalone Gmail application on a mobile device. *Id*. Samsung instead relies on a raft of extrinsic evidence. *See id*. at 68-69 (citing Ex. 1008, Ex. 1009, Ex. 1010, Ex. 1013). This deficiency alone renders Samsung's anticipation Ground 3A without merit.

To the extent the Director does find the Google blog article teaches a mobile phone web browser or a standalone Gmail application on a mobile device (it does not), both of Samsung's invalidity theories still fail to satisfy the Challenged Claims. These alleged local applications for accessing Gmail do not satisfy the following claimed requirements for a local application on a mobile device:

1) a user sets a desired security level configuration setting ***in the local application*** for the mobile device;[1]

---

[1] '347 Patent at 24:23-25 (Claim 1) ("enabling a user to set a desired security level configuration setting in the local application for the mobile device"), 24:54-57 (Claim 6) ("the local application including a first interface enabling a user to set a

2) the user is required to perform an authentication process before allowing access to the at least one feature of ***the local application***;[2]

1. The *Google* Blog Article Cannot Anticipate the Challenged Claims Because Petitioner Relies on a Combination of References (Ground 3A)

Samsung's anticipation challenge in Ground 3A fails because the Google blog article, as a single reference, fails to disclose each and every limitation of the Challenged Claims. Under 35 U.S.C. § 102, anticipation exists when a single piece of prior art satisfies, either expressly or inherently, every limitation of the claimed invention. *King Pharms., Inc. v. Eon Lab'ys, Inc.*, 616 F.3d 1267, 1274 (Fed. Cir. 2010). In this case, the Google blog article fails to satisfy "launching a local

---

desired security level configuration setting in the local application for the mobile device").

[2] '347 Patent at 24:32-35 (Claim 1) ("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"), 24:61-66 (Claim 6) ("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").

application on a mobile device" (Claim 1) or "a local application on a mobile device" (Claim 6).

Samsung notes the Google blog article's mention of a "Gmail account" and asserts Gmail can be accessed using "an internet browser on a mobile device" or "a standalone Gmail application on a mobile device." *Google* at 1; Pet. at 68, 70-71. But Samsung cannot cite to any portion of the Google blog article that mentions a mobile phone web browser or a standalone Gmail application on a mobile device.[3] Pet. at 68, 71. Samsung instead relies on a raft of extrinsic evidence to fill in the missing "local application on a mobile device" limitation. *See id*. at 68-69 (citing Ex. 1008, Ex. 1009, Ex. 1010, Ex. 1013). This is improper in making a challenge under 35 U.S.C. § 102.

A prior art reference only anticipates a patent's claim under § 102 "when the four corners of [that] . . . document describe every element of the claimed invention,

---

[3] The Google blog article mentions a "choice to generate the code for yourself using a mobile application on your Android, Blackberry, or iPhone device," but the context of this sentence indicates that "mobile application" refers to an authenticator application, such as Google Authenticator (and not a web browser or standalone Gmail application) used to generate the two-factor authentication code. *Google* at 1.

either expressly or inherently, such that a [POSITA] could practice the invention without undue experimentation." *Spansion, Inc.*, 629 F.3d at 1356 (cleaned up). "If it is necessary to reach beyond the boundaries of a single reference to provide missing disclosure of the claimed invention, the proper ground is not § 102 anticipation . . . ." *Scripps Clinic & Rsch. Found. v. Genentech, Inc.*, 927 F.2d 1565, 1577 (Fed. Cir. 1991), overruled on other grounds, *Abbott Lab'ys v. Sandoz, Inc.*, 566 F.3d 2009 (Fed. Cir. 2009).

Here, Samsung improperly seeks to combine or incorporate subject matter of extrinsic evidence (Exs. 1008, 1009, 1010, 1013) without showing it would have been obvious for a POSITA to combine the extrinsic evidence with the Google blog article to yield the claimed invention. Nor does Samsung provide the extrinsic evidence to prove the primary reference contains an enabled disclosure, to explain the meaning of a term used in the primary reference, or to show that a characteristic not disclosed in the reference is inherent. *See* MPEP § 2131.01 (discussing when multi-reference anticipation has been held proper). Here, Samsung has failed to show the Google blog article teaches every element of the claimed invention, including the requisite "local application on a mobile device."

"In an inter partes review . . . , the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence." 35 U.S.C. § 316(e). "Failure to prove the matter as required . . . means that the party with the burden of persuasion loses on that point . . . ." *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015). In this case, if any evidence existed that showed release dates and functionality for a standalone Gmail mobile application at the time the invention was made (July 18, 2011), Samsung could have produced and cited such documentation. Since it is Samsung's burden to show where the prior art teaches the claimed invention, the Director should infer that the evidence does not exist or does not say what Samsung alleges it discloses.

To the extent the Director does find the Google blog article teaches a mobile phone web browser or a standalone Gmail application on a mobile device (it does not), Samsung's mapping of these applications to the Challenged Claims is still flawed. A mobile phone web browser accessing Gmail and a standalone Gmail application still fail to satisfy the requirements of the Challenged Claims, for the below reasons.

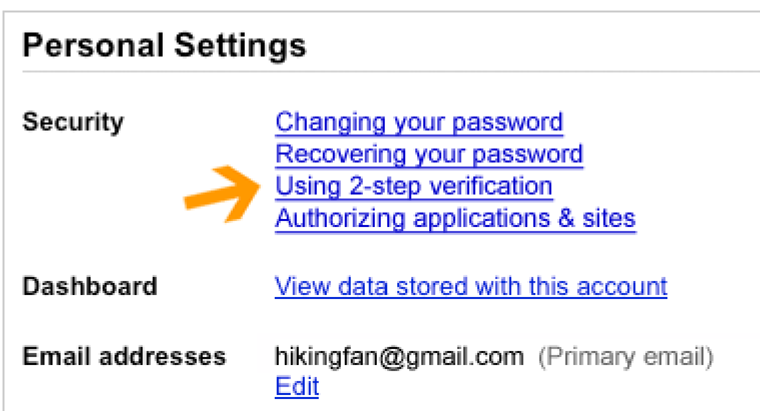
2. Gmail is Not a Feature of a Web Browser (Grounds 3A-3B, 4)

Samsung argues that the Google blog article discloses limitation [1d], including "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" because the Google blog article allegedly discloses "the user will be prompted to perform an authentication process before accessing Gmail's contents ('at least one feature of the local application')." Pet. at

75-76; '347 Patent at 24:32-35 (Claim 1), 24:62-66 (Claim 6). But this argument is flawed because Gmail is not a feature of a mobile device web browser (the alleged "local application on a mobile device" under one of Samsung's theories). Samsung acknowledges that Gmail is a ***web-based*** email service, which a POSITA understands is a web application stored and executed on a remote server (and not locally on the mobile device). Pet. at 68 (citing Ex. 1008 at [0022]). Samsung cites to its expert's testimony, but the expert declaration merely parrots the Petition and fails to support or explain how Gmail is a "feature" of a web browser, and not of Google's web applications. *Id*. at 75 (citing Cockburn ¶ 242).

3. Google Account Settings Page Are Not Set By a Standalone Gmail Application (Grounds 3A-3B, 4)

Samsung argues that the Google blog article discloses limitation [1b], including "enabling a user to set a desired security level configuration setting ***in the local application for the mobile device***" because the Google blog article discloses "a user may access an 'Account Settings page,' which 'looks like this:'"



Pet. at 72-74; '347 Patent at 24:32-35 (Claim 1) (emphasis added), 24:62-66 (Claim 6).

Samsung's argument is flawed because there is no evidence in the Google blog article that this cited "Account Settings page" is part of any standalone Gmail mobile application (the alleged "local application on a mobile device" under the second of Samsung's theories.). The claims require the desired security level configuration setting is set "***in the local application for the mobile device***." '347 Patent at Claim 1 ("enabling a user to set a desired security level configuration setting in the local application for the mobile device") (emphasis added). In fact, the Google blog article provides a hyperlink for the "Account Settings page" with the URL: https://www.google.com/accounts/ManageAccount, which is a webpage presumably for managing a Google Account, and not part of a local application.

Samsung's alternative argument, that "[t]o the extent not disclosed, a POSITA would have been motivated to modify the Gmail mobile application to allow access to *Google's* Account Settings," is pure hindsight. Pet. at 73. Petitioner alleges without evidence that the proposed change would "improve a user's experience, by placing all related functionality in a single location (i.e., the mobile application)." *Id*. Under *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355 (Fed. Cir. 2016), however, the use of "common sense" in a single-reference obviousness analysis should not be used "to supply a missing claim limitation" and should only be invoked when "the limitation in question was unusually simple and the technology particularly straightforward." *Id*. at 1361-62.

Samsung's argument also contradicts the record evidence. The Google blog article is not about securing Gmail accounts, it is about securing "Google Accounts." *Google* at 1. Samsung's own exhibits also show that a user's Google Account is responsible for providing access to ***multiple*** web-based services, not just Gmail. Ex. 1014 at 30:61-65 ("a Google Account [is] for accessing one or more web based services such as Gmail, Google calendars, Google reader, etc."). For this reason, Google maintains a single centralized location (i.e., the centralized "Account Settings" webpage found at: https://www.google.com/accounts/ManageAccount), rather than duplicate this account management functionality across various mobile applications. To this day, the Google Account Settings webpage, and not a local application on a mobile device, remains the centralized location for configuring security settings for a user's Google Account.

Meanwhile, Samsung provides no support, beyond mere attorney argument, that its proposed change would "improve a user's experience" and "encourage adoption of 2-step authentication." Pet. at 73-74. Samsung's expert declaration again merely parrots the Petition's conclusory assertions and does not provide substantial evidence for finding a motivation to combine. Cockburn ¶¶ 239-240.

Accordingly, Samsung has failed to establish that the Google blog article, alone or in combination with *Carter*, discloses the requisite "local application on a mobile device."

VI. CONCLUSION

For all of these reasons, PayGeo requests that the Director deny institution of *inter partes* review of the Challenged Claims of the '347 Patent.

Respectfully submitted,

Date: January 7, 2026

/James Hannah/

James Hannah (Reg. No. 56,369)
HERBERT SMITH FREEHILLS
KRAMER (US) LLP
333 Twin Dolphin Drive, Suite 700
Redwood Shores, CA 94065
Telephone: (650) 752-1700
james.hannah@hsfkramer.com

Jeffrey H. Price (Reg. No. 69,141)
Jeffrey Eng (Reg. No. 63,189)
Jenna Fuller (Reg No. 74,212)
HERBERT SMITH FREEHILLS
KRAMER (US) LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-9100
jeffrey.price@hsfkramer.com
jeffrey.eng@hsfkramer.com
jenna.fuller@hsfkramer.com

Attorneys for Patent Owner
PayGeo, LLC

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

The undersigned hereby certifies that the portions of the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** has 5,536 words in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using the Microsoft Word word-processing system used to prepare this paper.

Dated: January 7, 2026

/James Hannah/
James Hannah (Reg. No. 56,369)

Attorneys for Patent Owner
PayGeo, LLC

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), and pursuant to agreement by the parties that filing with the Board through the Patent Trial and Appeal Case Tracking System (P-TACTS) constitutes electronic service, service was made on Petitioners as detailed below.

Date of service	January 7, 2026
Manner of service	Electronic Filing with the Board (joshua.goldberg@finnegan.com; benjamin.saidman@finnegan.com; nicholas.cerulli@finnegan.com; alexander.boyer@finnegan.com; christina.yang@finnegan.com; christopher.anderson@finnegan.com; connor.mcgregor@finnegan.com)
Documents served	PATENT OWNER'S PRELIMINARY RESPONSE
Persons Served	Finnegan, Henderson, Farabow, Garrett & Dunner, LLP: Joshua L. Goldberg Benjamin A. Saidman Nicholas A. Cerulli Alexander M. Boyer Christina Ji-Hye Yang Christopher B. Anderson Connor M. McGregor

/James Hannah/
James Hannah
Registration No. 56,369
Lead Counsel for Patent Owner