

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

PROXENSE, LLC,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Civil Action No. 6:23-cv-320

JURY TRIAL REQUESTED

GOOGLE’S FINAL INVALIDITY CONTENTIONS

I. INTRODUCTION

Defendant Google LLC (“Google”) provides these Final Invalidity Contentions to Plaintiff Proxense, LLC (“Proxense”) for the following patents (collectively, “Asserted Patents” or “Patents-in-Suit”) and claims (collectively, “Asserted Claims”) identified as asserted in Plaintiff’s Preliminary Infringement Contentions served on July 24, 2023 (“Infringement Contentions”):

- U.S. Patent No. 8,352,730 (“the ’730 Patent”), claims 1-3, 5, and 15-17 (“the ’730 Asserted Claims”);
- U.S. Patent No. 8,886,954 (“the ’954 Patent”), claims 1-3, 5-7, and 22-27 (“the ’954 Asserted Claims”);
- U.S. Patent No. 9,298,905 (“the ’905 Patent”), claims 1-2, 4-5, 7, 15 (“the ’905 Asserted Claims”);
- U.S. Patent No. 8,646,042 (“the ’042 Patent”), claim 10 (“the ’042 Asserted Claim”);
- U.S. Patent No. 9,679,289 (“the ’289 Patent”), claims 14 and 16 (“the ’289 Asserted Claims”);
- U.S. Patent No. 10,073,960 (“the ’960 Patent”), claims 14 and 16 (“the ’960 Asserted Claims”);

The '730, '954, and '905 patents are collectively referred to herein as the "Device ID Patents." The '042, '289, and '960 Patents are collectively referred to herein as the "Hybrid Device Patents."

Google addresses the invalidity of the Asserted Claims and concludes with a description of its document production and identification of additional reservations and explanations.

II. RESERVATIONS AND EXPLANATIONS

These Final Invalidity Contentions and accompanying document productions are subject to further revision as follows. Nothing in these contentions constitutes an admission concerning the priority date, conception date, or date of reduction to practice of the Asserted Claims. Google reserves the right to modify or supplement these Invalidity Contentions, including in response to any positions taken or information disclosed regarding the priority date, conception date, or date of reduction to practice of the Asserted Claims. This disclosure is directed to invalidity issues only and does not address claim construction, non-infringement, patent misuse, inequitable conduct, or other non-statutory defenses. Google reserves all rights with respect to such issues, including but not limited to their position that the Asserted Claims are to be construed in a particular manner and are not infringed.

These Invalidity Contentions are based on Google's current knowledge, understanding, and belief as to the facts and information available as of the date of these contentions. Google has not yet completed its investigation, discovery, or analysis of information related to this action, and additional discovery may require Google to supplement or amend its Invalidity Contentions. Google reserves the right to amend or supplement its contentions once it gains access to relevant materials Proxense has not yet produced. While Google has made a good-faith effort to provide a comprehensive list of prior art relevant to this case, Google reserves the right to modify or further supplement its prior art list and contentions on invalidity of the Asserted Claims at a later time

with or based upon pertinent information that may be subsequently discovered from Proxense or third parties. Moreover, discovery is ongoing and Google reserves the right to pursue all other defenses that may be available to it, including but not limited to defenses that the Asserted Patents are unenforceable based on patent misuse, inequitable conduct, laches, estoppel, waiver, acquiescence, patent exhaustion, unfair competition, unclean hands, express or implied license, or any other grounds.

Any invalidity analysis depends on claim construction, which is a question of law reserved for the Court. Google reserves the right to amend, supplement, or materially modify its Invalidity Contentions in response to any claim construction positions that Proxense may take in this case or any claim construction the Court may adopt in this case. Google also reserves the right to assert that a claim is indefinite, not enabled, or fails to meet the written description requirement, in response to any additional claim construction positions Proxense may take in this case or any further claim construction the Court may adopt in this case. These disclosures are based on the apparent claim construction positions taken by the parties and the Court's constructions to date. These disclosures are not, and nothing in these disclosures should be seen as, an endorsement, acquiescence, or acceptance of any of Proxense's claim constructions.

Google's Final Invalidity Contentions are directed to the claims that are asserted and identified in Proxense's Infringement Contentions. Google reserves the right to modify, amend, supplement or otherwise alter its Invalidity Contentions in the event that Proxense supplements or amends its Infringement Contentions, takes a claim construction position that is different from or in addition to those seemingly set forth in its Infringement Contentions, or for any other reason.

Google further contends that Proxense appears to be pursuing overly broad constructions of the Asserted Claims in an effort to piece together an infringement claim where none exists and

to accuse products that do not practice the claims as properly construed. At the same time, Proxense's Infringement Contentions are in many respects too general and vague to discern exactly how Proxense contends the accused instrumentalities practice each element of the Asserted Claims. These Invalidity Contentions are not intended to be, and are not, an admission that the Asserted Claims are infringed by any of Google's products or technology, that any particular feature or aspect of the accused instrumentalities practices any element of the Asserted Claims, or that any of Proxense's proposed constructions are supportable or proper. To the extent that any of the prior art references disclose the same functionality or feature of any of the accused instrumentalities, Google reserves the right to argue that said feature or functionality does not practice the Asserted Claims, and to argue, in the alternative, that if said feature or functionality is found to practice the Asserted Claims, then the prior art reference demonstrates that that feature or functionality is not novel, is obvious, or is not patentable.

Attached hereto as Exhibit Nos. 730-01-43 and B, 954-01-44 and B, 905-01-44 and B, 042-01-31 and B, 289-01-31 and B, and 960-01-310 and B are representative claim charts that demonstrate how the Asserted Claims are invalid in view of certain prior art. Exhibit Nos. 730-01-43, 954-01-44, 905-01-44, 042-01-31, 289-01-31, and 960-01-31 provide examples of prior art that discloses, either expressly or inherently, or renders obvious every limitation of certain claims and/or teachings, suggestions and motivations through which a POSITA at the time of the alleged invention would have considered the limitations obvious in view of the state of the art at the time, the differences between the claimed invention and the state of the art, and the foreseeability from a technical perspective and/or marketing and/or natural and expected evolution of the art. Where Google cites a particular figure in a reference, the citation should be understood to encompass the caption and description of the figure and any text relating to the figure. Conversely, where Google

cites a particular text referring to a figure, the citation should be understood to include the figure as well. The references cited in the attached claim charts may disclose the limitations of the Asserted Claims expressly and/or inherently. Moreover, the suggested obviousness combinations are in the alternative to Google's contentions regarding anticipation. These obviousness combinations should not be construed to suggest that any reference included in any combination is not anticipatory in its own right.

For prior art patents and prior art publications identified in these Invalidity Contentions, Google reserves the right to rely on the public use, offer for sale, sale, and/or actual products embodying the methods and systems described therein uncovered during discovery. Google also reserves the right to rely on any related patents and patent applications, foreign patent counterparts and foreign patent applications of U.S. patents identified in these Invalidity Contentions, and U.S. counterparts of foreign patents and foreign patent applications identified in these Invalidity Contentions.

Google further reserves the right to rely on uncited portions of the prior art references and in other publications and testimony as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that a claim limitation is known or disclosed, whether expressly or inherently. Google further reserves the right to rely on uncited portions of the prior art references, other publications, and testimony to establish bases for combinations of certain cited references that render the Asserted Claims obvious.

Prior art not included in this disclosure, whether known or not known to Google, may be relevant to Google's invalidity arguments in this case. In particular, Proxense has not provided its contentions on validity of the Asserted Claims, and Google is currently unaware of the extent to which Proxense will contend that limitations of the Asserted Claims are not disclosed in the prior

art identified herein. Google reserves the right to identify, in response to Proxense's contentions, additional teachings in the same references or in other references that disclose or would have made the addition of the allegedly missing limitation obvious. Moreover, Google's search for prior art is ongoing, and Google has and will continue to subpoena third parties believed to have information relevant to this disclosure. Google expressly reserves the right to amend, supplement, or modify this disclosure as additional information is obtained from third parties, or from Proxense itself. Proxense also has a duty to produce to Google all relevant documents from other proceedings involving the patents related to the asserted patents or their subject matter, including but not limited to all prior art invalidity contentions and expert reports on invalidity among other relevant items.

Google reserves the right to modify, amend, or supplement these disclosures as additional information becomes available, and as its discovery and investigation proceeds.

III. PRIORITY DATE OF THE ASSERTED PATENTS AND CLAIMS

Proxense asserts that the '730 Patent, the '954 Patent, and the '905 Patent are entitled to a priority date of December 20, 2004, and the '042 Patent, the '289 Patent, and the '960 Patent are entitled to a priority date of December 6, 2007, in its July 24, 2023 Infringement Contentions.

It is Proxense's burden to show entitlement to its asserted priority dates, and Proxense has failed to meet that burden. *See Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1327 (Fed. Cir. 2008); *see also, In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1376 (Fed. Cir. 2016) ("[A] patentee bears the burden of establishing that its claimed invention is entitled to an earlier priority date than an asserted prior art reference."). For example, Proxense has failed to show that any of the Asserted Claims are entitled to a priority date earlier than the filing of the applications that issued as the asserted patents. Proxense therefore has not demonstrated that the patents are entitled to the dates of the provisional applications. Moreover, as addressed in more detail below, at least the '954 and '905 patents recite and claim subject matter not found in any early patents

and patent applications they claim priority to and thus those patents are not entitled to any priority date prior to December 10, 2012. Google reserves the right to amend its invalidity contentions with additional prior art and/or with additional charts of the art if Proxense changes its position and alleges earlier or later priority dates or if additional evidence demonstrates that the asserted patents are not entitled to their claimed priority dates. In addition, Proxense has not identified the date of conception for the patents-in-suit. Google therefore also reserves its right to amend its Invalidity Contentions if Proxense is permitted to allege earlier dates of conception for the patents-in-suit, or if Proxense does not meet its burden to prove the priority dates it asserts.

IV. BACKGROUND OF THE TECHNOLOGY AT ISSUE

A. '730/'954/'905 Patents (Device ID Patents)

The '730 Patent, the '954 Patent, and the '905 Patent relate generally to systems and methods for authentication. These patents acknowledge the existence of various existing methods of providing secure authentication, such by requiring a user to provide “secret credentials” before allowing access, requiring a unique “access object” such as a key, or “hybrid authentication techniques” that require both. '730 Patent at 1:23-48. The patents assert that “secret credentials” required users to “memorize or otherwise keep track of the[ir] credentials” and that “access objects” risked illegitimate users “us[ing] a stolen access object to enter a secured location because the user’s identity is never checked.” *Id.* The patents allegedly solve these purported problems by using a device ID code stored on the device and transmitted to a third party trusted authority in lieu of memorized secret credentials and ensuring the device has not been stolen via a biometric scan. These were all well-known concepts long before the priority dates of the Device ID Patents. *See, e.g.,* Menezes *et al.*, “Handbook of Applied Cryptography,” at 387 (1996) (“Menezes”), *available at*

<https://theswissbay.ch/pdf/Gentoomen%20Library/Cryptography/Handbook%20of%20Applied>

[%20Cryptography%20-%20Alfred%20J.%20Menezes.pdf](#) (addressing use of smart cards or IC cards and biometrics as alternatives to “standard passwords”). Software for securely storing passwords on a device to decrease the need to memorize the same has existed since at least the 1990s. <https://www.wired.com/1998/10/padlocking-windows-95/>. Using an object associated with a unique number, coupled with a secondary form of authentication to ensure the object has not been stolen, is also the basic concept underpinning debit cards and ATMs since at least the 1960s. *See* Menezes at 25 (“Person A provides to a banking machine a personal identification number (PIN) along with a magnetic stripe card containing information about A. The banking machine uses the information on the card and the PIN to verify the identity of the card holder.”); *id.* at 395 (“[A] common technique is for the PIN to serve to verify the user to the token, while the token contains additional independent information allowing the token to authenticate itself to the system (as a valid token representing a legitimate user).”); U.S. Pat. No. 3,543,904; U.S. Pat. No. 3,761,682. Indeed, by the alleged priority date of the Device ID patents, biometric authentication to protect access to cell phones was well known, including cell phones with mobile wallet applications installed thereon that could be used as replacements for credit cards – the very technology now accused of infringement by Proxense. *See* Exhibits 730-34, 905-34, and 954-34.

Moreover, as addressed below, the ’954 and ’905 patents are not even entitled to a December 20, 2004 filing date, and instead are at best entitled to the December 10, 2012 filing date of the application for the ’954 patent. By that time, cell phones with biometric authentication and mobile payment applications were well known in the art thanks to work by Google. By 2011, cell phones were available running the Google Android Operating System that supported biometric authentication, including the Motorola Atrix. Marc Saltzman, “Motorola

Atrix 4G Review” (March 16, 2011), *available at* <https://www.digitaltrends.com/mobile/motorola-atrrix-4g-review/>; Shane Conder, “Enable Fingerprint Scanner for Android on the Motorola ATRIX 4G” (Sept. 26, 2011), *available at* <https://www.developer.com/mobile/enable-a-fingerprint-scanner-for-android-on-the-motorola-atrrix-4g/>. In addition, in 2011, Google released a “Google Wallet” application that allowed users to save their credit card to their phone and then use their phone to make purchases at stores via wireless NFC technology. MG Siegler, “Google Unveils Wallet and Offers: An Open Platform For Mobile Payments” (May 26, 2011), *available at* <https://techcrunch.com/2011/05/26/google-wallet-offers/>; <https://www.youtube.com/watch?v=am8t6iZ7up0&t=50s/>. The initial version stored the credit card number in encrypted form on the phone, while a later version released in August 2012 stored a virtual or proxy card (also called “wallet ID”) which is then translated to a credit card number by backend servers. Google Commerce Blog, “Use any credit or debit card with Google Wallet” (August 1, 2012), *available at* <https://commerce.googleblog.com/2012/08/use-any-credit-or-debit-card-with.html>; *see also* <https://arstechnica.com/gadgets/2014/10/how-mobile-payments-really-work/2/>; <https://stackoverflow.com/questions/19525166/google-wallet-for-digital-goods-api-vs-google-play-in-app-billing>.

Thus, each of the steps recited in these patents claims, including biometric authentication, device ID code, third party trusted authority, memory that cannot be subsequently altered, and access message were all well-known to the public long before the purported December 2004 priority date of these patents. Google incorporates by reference the prior art disclosure in Exhibit Nos. 730-01-43 and B, 954-01-44 and B, 905-01-44 and B.

1. Biometric Authentication

The '730 Patent, the '954 Patent, and the '905 Patent claim the use of biometric verification, which “uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner.” '730 patent at 2:62-64. However, even the patents themselves admit that “[c]onventional techniques for comparing fingerprints can be used.” '730 patent at 4:19-20.

Historically, authentication methods have fallen into three categories: “something the user has, something the user knows, or something the user is.” Hansen, “Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust,” at 15 (1999). Biometrics as a concept for identifying individuals or verifying their identity through “something the user is” has existed for centuries. Mark Twain included a chapter titled “A Thumb-Print and What Came of It” in his 1883 memoir “Life on the Mississippi,” where he addressed the unique nature of thumb prints and how they can be used for identification.

<https://www.telelib.com/authors/T/TwainMark/prose/lifeonmississippi/lifeonmississippi31.html>.

In the 1960s and 1970s, the FBI contracted with the National Institute of Standards and Technology (NIST) to study the process of automating fingerprint identification and subsequently funded the development of fingerprint scanners for automated classifiers, resulting in the development of the M40 algorithm and Automated Fingerprint Identification Systems (AFIS). https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf. By 1996, fingerprint scanners and biometric verification were so ubiquitous to the public consciousness that they were referenced in Mission Impossible:



Mission Impossible, 1996, character Sarah Davies bypassing a fingerprint scanner.



Mission Impossible, 1996, character Ethan Hunt using a retina scanner.

By 2001, fingerprint scanners were being included in commercially available laptops, such as the Acer TravelMate 739TLV and Compaq Armada E500.

<https://www.cnn.com/2001/TECH/computing/02/02/biometric.security.idg/index.html>. Before the December 2004 claimed priority date of the patents, fingerprint scanners had even been integrated into cell phones, including the SAGEM MC 959 in 2000

(<https://www.telecompaper.com/news/sagem-launches-mc-959-id-dual-band-gsm-handset--207905>), Fujitsu F505i in 2003

(https://blog.greggman.com/blog/cell_phone_thumbprint_sensor/), and Pantech GI100 in 2004

(<https://www.engadget.com/2004-08-03-stick-em-up-a-pantech-gi100-then-gimme-your-phone-and-your.html>).

2. Device IDs, Passkeys, and Tokenization

The '730 Patent, the '954 Patent, and the '905 Patent claim the use of a device ID that “uniquely identif[ies] the integrated device.” '730 Patent at claim 1; '954 Patent at claim 1; '905 Patent at claim 1.

Unique device identifiers have been publicly known for decades. Unique MAC addresses were part of the IEEE 802.3 Ethernet standard since the first iteration in 1985 and are transmitted as part of each frame. <https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub107-Mar1985.pdf> at 23-26 (frames include 48-bit addresses “specify the destination addressee(s)” and “identify the station from which the frame was initiated”). The IEEE Registration Authority is responsible for allocating these unique MAC addresses. <https://standards.ieee.org/wp-content/uploads/import/ieemacaddress.png>. Universally Unique Identifiers (UUIDs), also called Globally Unique Identifiers (GUIDs), have also been in use since at least 1990 and were standardized in an IETF draft starting in October 2002. <https://datatracker.ietf.org/doc/html/draft-mealling-uuid-urn-00> at Abstract (“A UUID is 128 bits long, and if generated according to the one of the mechanisms in this document, is either guaranteed to be different from all other UUIDs/GUIDs generated until 3400 A.D. or extremely likely to be different (depending on the mechanism chosen). UUIDs were originally used in the Network Computing System (NCS) [1] and later in the Open Software Foundation’s (OSF) Distributed Computing Environment [2].”). Using such unique Device IDs to control access, such as configuring a DHCP server to only grant access to MAC addresses appearing on a list of authorized devices, was also known. <https://bbs.archlinux.org/viewtopic.php?id=7273>.

Proxense in its infringement contentions further alleges that “passkeys” meet the “device ID code” limitation. Ex. A1 at 5. A passkey is used to generate an encrypted signature, and such use of encrypted signatures has also been known long before the priority date of Proxense’s patents. By 1991, “[a] widely adopted” authentication method was “authenticating data as an encryption formula or cryptokey.” Coley, “User Authentication: A State-of-the-Art Review,” at 65-66 (1991). The user generates an encrypted reply to a host’s random challenge that is then used to control access to a system. *Id.* The host determines which user is attempting to access the system based on the encrypted reply. *Id.*

As another example, the 1996 textbook “Handbook of Applied Cryptography” teaches using keys to generate “digital signatures.” Menezes at 425 (“This chapter considers techniques designed to provide the digital counterpart to a handwritten signature. A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed.”). As the textbook recognizes, such use of “digital signatures” is often coupled with the “certification public keys” by “a trusted third party (TTP).” This use of trusted third parties is discussed in more detail below in connection with the claimed “third party trusted authority.”

Proxense in its infringement contentions further alleges that “EMV payment tokens” meet the “device ID code” limitation. Ex. A2 at 3. In tokenization, a non-sensitive surrogate value is used in lieu of sensitive data. This concept long predates Proxense’s patents. For example, in the physical world, “coin tokens have a long history of use replacing the financial instrument of minted coins and bank notes.” Rolfe, “The fall and rise of Tokenization,” at 1 (2015). And similarly, in the digital setting, “surrogate key values have been used since 1976 to isolate data associated with the internal mechanisms of databases and their external equivalents

for a variety of uses in data processing.” *Id.* at 1; *see also* Nijssen, G.M., *Modelling in Data Base Management Systems* (1976). Indeed, by 2001, tokenization was not just readily known, but was even being applied in commercial systems (e.g., by a company called TrustCommerce) to replace primary account numbers (PANs) with randomly generated tokens – *i.e.*, the “payment tokens” that Proxense is now alleging meet the “device ID code” limitation.

<https://web.archive.org/web/20010405203446/https://trustcommerce.com/billing.html> (replacing “billing information” with “[a] six-digit alphanumeric billing ID”; customer billing information is then securely stored “in the TrustCommerce database,” while merchants use the “billing ID ... to run transactions”).

3. Memory That Cannot Be Altered / Temper Proof

The ’730 and ’954 Patents also claim storing biometric data and the device ID code in “a tamper proof format” and within “a storage element on the integrated device that is unable to be subsequently altered.” The patents explain that this is done via “a memory element that can be written to once but cannot subsequently be altered,” such as “a ROM element, a flash memory element, or any other type of non-volatile storage element.” ’730 Patent at 4:29-42. Such use of read-only memory (ROM) has existed for decades.

For example, an article published at the Computer History Museum describes that the first 256-bit and 1024-bit read-only memory (the type of memory described in the Device ID Patents as allegedly resulting in a tamper proof format and storage of data that cannot be subsequently altered) were invented as early as 1965 by Sylvania and General Microelectronics. Computer History Museum, “1965: Read-Only-Memory Chips Appear,” at 1. Later, “[b]y the early 1970s Fairchild, Intel, Motorola, Signetics, and TI offered 1024-bit TTL ROMs, while AMD, AMI, Electronic Arrays, General Instrument, National, Rockwell and others produced 4096-bit (4K) MOS devices.” *Id.*

Additionally, in a 1965 publication, Morton H. Lewin describes multiple forms of read-only memories, including various linear and non-linear arrays and optical systems. *See generally* Lewin, “A Survey of Read-Only Memories” (1965). Lewin specifies that “read only memory systems vary from those in which information stored is more or less absolutely fixed (or at least changed with great difficulty) to those in which information can be changed at slow electronic speeds.” *Id.* at 784.

4. Third-Party Trusted Authority and Public Key Infrastructure

The '730 Patent, the '954 Patent, and the '905 Patent all claim a “third party trusted authority.” Trusted third parties have been used in cryptography for decades. Indeed, the textbook “Handbook of Applied Cryptography” from 1996 has an entire section dedicated to “Trusted third parties and public-key certificates.” Menezes at 39. This concept is also sometimes referred to as “public key infrastructure” or “PKI” and has been around since at least 1976 (“New Directions in Cryptograph,” Whitfield Diffie and Martin Hellman, IEEE Transactions on Information Theory, 1976.), and RSA (Rivest-Shamir-Adleman) technology (an example of PKI) still used today was published in 1978 (Ronald Rivest, Adi Shamir, and Leonard Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Communications of the ACM, 1978). Also in 1977, the National Institute of Standards and Technology (NIST) published the Data Encryption Standard (DES). Federal Information Processing Standard (FIPS) Publication 46, The Data Encryption Standard (DES), 1977. By 1998, this authentication framework—and the associated definition of a Certification Authority—was standardized as X.509, and such use of a third party trusted authority was commonplace in the 1990s. CCITT, “Series X: Data Communication Networks: The Directory – Authentication Framework” (Nov. 1988); <https://datatracker.ietf.org/doc/html/rfc2459>; <https://datatracker.ietf.org/doc/html/rfc1422>.

There are many other examples of publications much older than the asserted patents describing the claimed “third party trusted authority.” For example, in his 1994 dissertation, Proxense’s expert, Avial David Rubin, describes that “the use of cryptography for secrecy, integrity, and authentication in a distributed system requires an environment in which each principal is in possession of a secret key. This is called an authenticated environment. Depending on the type of cryptography in use, each principal may also have a public key.” Rubin, “Nonmonotonic Cryptographic Protocols,” at 2 (1994). Rubin further describes that for a principal in a distributed system to prove its identity, “typically, each principal shares a secret with some trusted machine, called an authentication server.” *Id.* at 23. This shared secret is “typically used as an encryption key.” *Id.* at 24. In this scheme, “a user cannot generate or decrypt encrypted data without possession of the key. Thus, a principal proves it is in possession of a key by encrypting with it.” *Id.* at 24. Rubin even discusses an existing example, the Kerberos authentication system developed at MIT, in which “each principal shares a secret encryption key with the Kerberos server, a machine that must be kept physically secure.” *Id.* at 2.

In another example, in his 1999 thesis, Anthony P. Hansen discusses public key infrastructures, which are “the underlying system[s] comprised of the applications, policies, standards and laws that governs the generation, storage, distribution and management of both cryptographic keys and digital certificates.” Hansen, at 4. He discusses “[t]wo key, public key or asymmetric key cryptosystems,” which are “characterized by two different keys, E_k and D_k .” *Id.* at 29. In these systems, “[t]he public key gets its name because it is distributed so that everyone has easy access to it. The public key is used for encryption and anyone can use it. The private key is necessary for decryption and must be kept secret to ensure confidentiality.” *Id.* at 29. Rubin also discusses asymmetric (public) key pairs, which are “pairs of keys that are

inverses of each other.” Rubin at 27. In these systems, “one key is kept private, and is known only to the principal who possesses it. The other key is public, and is made widely available.” *Id.* at 27. “Data encrypted with the private key can be decrypted with the public key; similarly, data encrypted with the public key can be decrypted with the private key.” *Id.* at 27. Thus, in these systems, both the private and the public key can be used to encrypt or decrypt, but one is “secret” and one is not. When implementing such asymmetric key pairs, a copy of the private key is “stored securely” by “a trusted third party such as an employer, a CA, or a government agency.” Hansen at 47. Further “[a]dditional security may be obtained by splitting the copy and storing it with multiple trusted third parties so no one third party has access to the key without complicity of the others.” *Id.*

5. Access Message

The ’730 Patent, the ’954 Patent, and the ’905 Patent all claim an “access message ... allowing the user access to an application” or “to complete a financial transaction.” ’730 patent claim 1; ’954 Patent claim 1; ’905 Patent. The concept of an access message that allows a user access existed long before the priority dates of these patents. For example, OnStar has been offering a remote unlock service for cars since at least 1996, which necessarily entails receiving an access message allowing access to the car.

<https://www.chicagotribune.com/1996/05/27/rescu-ford-vs-onstar-gm/>. By 2003, OnStar had processed at least “27,000 remote door-unlock requests.”

<https://www.electronicdesign.com/technologies/communications/article/21772352/onstar-system-puts-telematics-on-the-map>.

B. ’042/’289/’960 Patents (Hybrid Device Patents)

The ’042 Patent, the ’289 Patent, and the ’960 Patent are “generally relate[d] to personal digital keys and corresponding sensors, capable of proximity detection/location determination

and auxiliary data services/application services.” ’042 patent 1:21-27. These patents acknowledge that such proximity sensors and location tracking technologies existed at the time. ’042 patent 1:52-61. These patents propose combining such existing “personal digital key (PDK)” with equally known “receiver-decoder circuit (RDC)” to arrive at a “hybrid device,” i.e., putting two known circuits into a single box. ’042 patent 1:65-2:20. The claims further recite creating a wireless link between a PDK and RDC and also generating an enablement signal. However, each of these elements of the claimed invention (PDKs, RDCs, wireless links, and enablement signals) existed long before the claimed priority dates of the ’042 Patent, the ’289 Patent, and the ’960 Patent. Google incorporates by reference the prior art disclosures in Exhibit Nos. 042-01-31, B; 289-01-31, B; 960-01-31, B.

1. PDK

The asserted claims of the ’042 and ’289 Patents claim a “hybrid device,” that includes an “personal digital key” or “PDK.” The Court has construed the term “personal digital key” as “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.” Dkt. 59. Under this definition and Proxense’s apparent interpretation of the claims, personal digital keys have existed for years prior to the priority date of these patents.

For example, cell phones contain antennas and transceivers, as well as controllers and memories for storing personal information. The first cell phone that was available to the general public was first used in April 1973. McNamee, “50 years ago, Martin Cooper made the first cellphone call,” at 1 (2023). The very first smartphone was released by IBM in 1994, called the Simon Personal Communicator (SPC). Tocci, “Smartphone History and Evolution,” at 1 (2023). The SPC had the ability to send and receive emails and faxes, and also had a calendar, address book, and a native appointment scheduler. *Id.*

The patents themselves acknowledge several common applications in which PDKs (also called proximity sensors within these patents) were used to control access to resources “based on biometrics passwords, PINs, or other types of authentication. ’042 Patent at 1:29-37. In these previously existing use cases, a device containing a proximity sensor that stored personal information such as biometrics, passwords, and PINs, would be considered a personal digital key. The patents also provide the existing example of RFID, which would store the user’s location information and could interact with RFID readers to transmit that location information. ’042 Patent at 1:38-51. Indeed, patent applications by Proxense that qualify as prior art to the Hybrid Device Patents disclose PDKs. See U.S. Pat. Appl. Publ. No. 2007/0245157.

2. RDC

The asserted claims of the ’042 and ’289 Patents claim a “hybrid device,” that includes an “receiver-decoder circuit” or “RDC.” The Court has construed the term “receiver-decoder circuit” as “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.” Dkt. 59. Under this definition and Proxense’s apparent interpretation of the claims, receiver-decoder circuits have similarly existed for decades.

Devices for encryption and decryption of information can be traced back for hundreds of years. Morkel, “Encryption Techniques: a Timeline Approach,” at Abstract (2004). For example, Thomas Jefferson invented the first wheel cipher in the 1790s. *Id.* at 6. Enigma, the decryption machine used in World War II, was invented in 1923. *Id.* at 7. These early decryption methods lay the groundwork for modern cryptography implemented in electronic circuits after the first computers were created around 1943-1945. *Id.* at 7.

Technological advancements in electronics and computing gave rise to forms of data conversion, which implemented decoder circuits. Telegraphs, for example, consisted of

transmitters and receivers that decoded electronic signals into written messages.

<https://letstalkscience.ca/educational-resources/interactives/telegraph-key> at 7. The receiver on a telegraph therefore "receives data in an encrypted format and decodes the encrypted data for processing." *Id.*

Another early example of a receiver-decoder circuit under the Court's construction would be receivers in radio communications. During World War II, one of the first secure speech systems was implemented in German communications, called SIGSALY. Weadon, "NSA SIGSALY Story," accessible at <https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/wwii/sigsaly-s%E2%80%A6> at 1. SIGSALY worked by adding a noise filter on top of a voice message, thereby encrypting the voice message.

<https://99percentinvisible.org/episode/vox-ex-machina/> at 2. When the encrypted voice message was received on the other end, the noise would be removed, thereby decrypting the message. Thus, the SIGSALY receiver would wireless receive data in an encrypted format and decode the encrypted data for processing.

Indeed, patent applications by Proxense that qualify as prior art to the Hybrid Device Patents disclose RDCs. *See* U.S. Pat. Appl. Publ. No. 2004/0255139.

3. Wireless Links

The asserted claims of the '042 Patent, the '289 Patent, and the '960 Patent all require creating a "wireless link." But wireless links have existed for more than a century. In 1849, when Heinrich Hertz demonstrated the transmission of electromagnetic waves through space. Fahim at 1. Since then, other forms of wireless communications have become ubiquitous, including radio and telephone. *Id.* Examples of known technologies for creating a wireless link include Bluetooth, originally conceived by Ericsson in 1994 (NIST Guide to Bluetooth Security 800-121 Revision 2 (2017) at 3), Infrared Data Association (IrDA), established in 1993 (Vishay,

“Infrared Data Communication According to IrDA Standard,” at 1), and Wi-Fi, released by the IEEE in 1997 as 802.11-1997 (<https://purple.ai/blogs/history-wifi/> at 1).

4. Passkey Authentication

Proxense in its infringement contentions alleges that use of “passkeys” infringes the Hybrid Device Patents. Ex. D at 1-6. Such use of passkeys long predates the Hybrid Device Patents. *See supra* at Section IV.A.4.

5. Two-Factor Authentication

Proxense in its infringement contention alleges that using a second device to log into a first device infringes the Hybrid Device Patents. Ex. D at 5.¹ This concept of two-factor authentication long predates the Hybrid Device patents. For example, there are numerous companies already in the 1990s that were manufacturing tokens for two-factor authentication, whereby a user would use a code shown on the token or smart card to log into an account. <https://apps.dtic.mil/sti/tr/pdf/ADA318942.pdf> at 17-19.

As another example, in 1998, AT&T received a patent on alerting a customer via pager of a transaction and requiring the customer to approve the transaction on that pager. U.S. Pat. No. 5,708,422 at Abstract (“[A] request to authorize the transaction is received, wherein the request includes a customer identifier; a determination is made whether to authorize the transaction based on the customer identifier; if the determination is to authorize the transaction, that fact is communicated to the customer; a confirmation that the transaction should, in fact, be authorized is received back from the customer; and the transaction is authorized in response to the customer’s confirmation thereof. ... A preferred method of alerting the customer and receiving a confirmation to authorize the transaction back from the customer is illustratively afforded by

¹ In addition, because Proxense accuses the concept of using a phone to log into an account of infringing the Device ID patents, this section is equally applicable to the Device ID patents.

conventional two-way pagers.”). AT&T’s patent further recognized that “the principles of the present invention may be applied to a wide variety of transactions including, but not limited to, ... secure access transactions such as computer access transactions based on computer passwords.” *Id.* at 15:61-16:3. The patent also explains that its teachings are also applicable to, e.g., “cellular telephones” instead of pagers. *Id.* at 16:14-22.

V. PRIOR ART REFERENCES

Google identifies the following prior art now known to Google to anticipate or render obvious the Asserted Claims under at least 35 U.S.C. §§ 102(a), (b), (e), and/or (g), either expressly or inherently as understood by a POSITA, and/or rendered obvious under 35 U.S.C. § 103, either alone or in combination. At this time, Google contends that the following prior art references described below anticipate or render obvious, either alone or in combination, one or more of the Asserted Claims of the ’730 Patent, the ’954 Patent, the ’905 Patent, the ’042 Patent, the ’289 Patent, and/or the ’960 Patent. These prior art references also provide a description of the level of skill in the art and provide background information showing the knowledge of a person of skill in the art. Google reserves the right to rely on these references for those purposes.

Google additionally incorporates by reference all prior art references cited on the face of the ’730 Patent, the ’954 Patent, the ’905 Patent, the ’042 Patent, the ’289 Patent, the ’960 Patent, related patents, and all foreign counterparts. Google further incorporates by reference all references identified in the file history of the same. Google further incorporates by reference all prior art references cited in all *inter partes* review and *ex parte* reexamination requests filed challenging the Asserted Patents and any related patents. *See, e.g.*, IPR2021-01438; IPR2021-01439; IPR2021-01444; IPR2021-01447; IPR2021-01448; IPR2024-00405; IPR2024-00407; IPR2024-00232; IPR2024-00233; IPR2024-00234; IPR2024-00573; Reexamination Nos. 90/015,052, 90/015,053, 90/015,054. Indeed, during *ex parte* reexamination the patent examiner

rejected all claims of the '905 Patent as unpatentable over prior art Ludtke, Okereke, and Robinson. Ex parte reexamination of U.S. Patent 9,298,905, Control No. 90/015,053, March 4, 2024 Final Rejection. Google reserves the right to rely upon foreign counterparts of the U.S. Patents identified in these invalidity contentions, U.S. counterparts of foreign patents and foreign patent applications identified in these invalidity contentions, U.S. and foreign patents and patent applications corresponding to articles and publications identified in these invalidity contentions, and any systems, products, or prior inventions related to any references identified in these invalidity contentions.

In these invalidity contentions, including the exhibits, any citation to a printed publication or other reference describing a prior art system should also be construed to include a reference to the prior art system itself.

A. '730/'954/'905 Patents (Device ID Patents)

1. Prior Art Patents and Publications

Prior Art Reference	Effective Filing Date	Publication Date
CA 2,335,532,A1 (De Schrijver)	26-Jun-99	6-Jan-00
CA 2,466,734,A1 (Samar)	22-Jan-03	31-Jul-03
EP 1,224,518,B1 (Vamvakas)	6-Oct-00	15-Jul-09
EP 1,470,534,B1 (Samar)	22-Jan-03	27-Oct-04
EP 1,536,306,A1 ('306 Buer)	30-Sep-04	1-Jun-05
EP 1,959,369,A1 (Takashi c/o Fujitsu Limited Shnzaki)	10-Dec-99	20-Aug-08
EP 2,797,020,A2(Buer)	30-Sep-04	29-Oct-14
EP 2,797,020,A3(Buer)	30-Sep-04	3-Sep-14
EP 2,937,805,A1 (Buer)	30-Sep-04	28-Oct-15
EP 3,023,899,A1 (Buer)	30-Sep-04	25-May-06
EP 3,023,899,B1 (Buer)	30-Sep-04	16-Sep-20
GB 2,353,386,A (Scott)	26-Apr-99	4-Nov-99
GB 2,353,386,B (Scott)	26-Apr-99	4-Nov-99
GB 2,401,462,A(Chen)	22-Apr-04	10-Nov-04
US 2001/0000535/A1 (Lapsley)	6-Dec-00	26-Apr-01
US 2001/0026632/A1(Tamai)	19-Mar-01	4-Oct-01
US 2001/0030644/A1(Allport)	5-Jun-01	18-Oct-01
US 2002/0003892/A1(Iwanaga)	9-Jul-01	10-Jan-02

US 2002/0046336/A1 (Kon)	30-Aug-01	18-Apr-02
US 2002/0099665/A1(Burger)	1-Oct-01	25-Jul-02
US 2002/0109580/A1 (Shreve)	13-Feb-01	15-Aug-02
US 2002/0116508/A1(Khan)	20-Feb-02	22-Aug-02
US 2002/0126780/A1(Oshima)	5-Dec-01	12-Sep-02
US 2002/0188574/A1 (Niwa)	29-Jul-02	12-Dec-02
US 2002/0194128/A1 (Maritzen)	27-Mar-02	19-Dec-02
US 2003/0037264/A1 (Ezaki)	13-Aug-02	20-Feb-03
US 2003/0051138/A1 (Maeda)	24-Jun-02	13-Mar-03
US 2003/0055792/A1 (Kinoshita)	23-Jul-01	20-Mar-03
US 2003/0074317/A1 (Hofi)	15-Oct-01	17-Apr-03
US 2003/0093693/A1 (Blight)	12-Nov-03	15-May-03
US 2003/0120934/A1 (Ortiz)	10-Jan-01	7-Sep-10
US 2003/0131114/A1 (Scheidt)	15-Oct-02	10-Jul-03
US 2003/0135740/A1 (Talmor)	5-Sep-01	17-Jul-03
US 2003/0140233/A1 (Samar)	22-Jan-02	24-Jul-03
US 2003/0154382/A1 (Vicard)	17-Jan-03	14-Aug-03
US 2003/0177102/A1 (Robinson)	21-Sep-01	18-Sep-03
US 2003/0196084/A1 (Okereke)	11-Apr-03	16-Oct-03
US 2003/0200446/A1 (Siegel)	19-Apr-02	23-Oct-03
US 2003/0220876/A1 (Burger)	19-Mar-03	27-Nov-03
US 2004/0014423/A1 (Croome)	14-May-03	22-Jan-04
US 2004/0044627/A1 (Russell)	29-Nov-00	4-Mar-04
US 2004/0123106/A1 (D'Angelo)	26-Aug-03	24-Jun-04
US 2004/0148526/A1 (Sands)	24-Jan-03	29-Jul-04
US 2004/0153649/A1 (Rhoads)	27-Jul-95	3-Aug-10
US 2004/0257196/A1 (Kotzin)	20-Jun-03	23-Dec-04
US 2005/0005136/A1(Chen)	21-Apr-04	6-Jan-05
US 2005/0039027/A1 (Shapiro)	25-Jul-03	17-Feb-05
US 2005/0091213/A1 (Schutz)	23-Oct-03	28-Apr-05
US 2005/0105734/A1 (Buer)	30-Sep-04	19-May-05
US 2005/0221798/A1 (Sengupta)	30-Mar-04	6-Oct-05
US 2005/0225430/A1 (Seifert)	19-Dec-02	13-Oct-05
US 2005/0253683/A1 (Lowe)	17-May-04	17-Nov-05
US 2006/0129838/A1 (Chen)	8-Aug-02	15-Jun-06
US 2006/0136741/A1 (Mercredi)	16-Dec-04	22-Jun-06
US 2006/0143441/A1 (Giobbi-441)	12-Dec-2005	29-Jun-2006
US 2007/0038867/A1 (Verbauwhede)	2-Jun-04	15-Feb-07
US 2010/0062743/A1 (Jonsson)	20-Aug-04	11-Mar-10
US 5,623,552,A (Lane)	15-Aug-94	22-Apr-97
US 5,867,795,A (Novis)	23-Aug-96	2-Feb-99
US 6,011,858,A (Stock)	10-May-96	4-Jan-00

US 6,016,476,A (Maes)	16-Jan-98	18-Jan-00
US 6,041,410/A (Hsu)	22-Dec-97	21-Mar-00
US 6,104,922,A (Baumann)	2-Mar-98	15-Aug-00
US 6,219,439,B1 (Burger)	9-Jul-98	17-Apr-01
US 6,325,285,B1 (Baratelli)	12-Nov-99	4-Dec-01
US 6,353,889,B1 (Hollingshead)	13-May-98	5-Mar-02
US 6,751,734,B1 (Uchida)	21-Mar-00	15-Jun-04
US 6,819,219,B1 (Bolle)	12-Oct-00	16-Nov-04
US 6,907,135,B2 (Gifford)	2-Mar-99	14-Jun-05
US 6,957,339,B2 (Shinzaki)	7-Jun-02	18-Oct-05
US 7,155,416,B2 (Shatford)	3-Jul-03	26-Dec-06
US 7,188,110,B1 (Ludtke)	11-Dec-00	6-Mar-07
US 7,200,755,B2 (Hamid)	24-May-01	3-Apr-07
US 7,249,112,B2 (Berardi)	13-Dec-02	24-Jul-07
US 7,310,042,B2 (Seifert)	19-Dec-04	18-Dec-07
US 7,404,086,B2 (Sands)	24-Jan-03	22-Jul-08
US 7,478,065,B2 (Ritter)	23-Dec-99	13-Jan-09
US 7,561,691,B2 (Blight)	12-Nov-01	14-Jul-09
US 7,636,854,B2 (Müller)	2-May-02	22-Dec-09
US 8,166,523,B2 (Ezaki)	13-Aug-02	24-Apr-12
US 8,232,862,B2 (Lowe)	17-May-04	31-Jul-12
US 8,333,317,B2 (Buer)	30-Sep-04	18-Dec-12
US 8,548,927,B2 (Beenau)	10-Jul-01	1-Oct-13
US 8200980,B1 (Robinson)	7-Jun-04	12-Jun-12
WO 00/00882/A2 (De Schrijver)	25-Jun-99	6-Jan-00
WO 00/00923/A1 (Valliani)	30-Jun-99	6-Jan-00
WO 01/027723/A1 (Vamvakas)	6-Oct-00	19-Apr-01
WO 01/27723/A1 (Vamvakas)	6-Oct-00	19-Apr-01
WO 02/089018/A1 (Pu)	2-May-01	7-Nov-02
WO 02/095547/A2 (Hamid)	23-Apr-02	28-Nov-02
WO 03/003295/A1 (Poo)	28-Jun-01	9-Jan-03
WO 03/036861/A1 (Black)	28-May-02	1-May-03
WO 03/054806/A2 (Seifert)	19-Dec-02	3-Jul-03
WO 03/063094/A2 (Samar)	22-Jan-02	31-Jul-03
WO 03/093923/A2 (Eryou)	30-Apr-03	13-Nov-03
WO 2004/019190/A1 (Chen)	8-Aug-02	4-Mar-04
WO 2004/068283/A2 (Sands)	23-Jan-04	12-Aug-04
WO 98/12670/A1 (Borza)	15-Sep-97	26-Mar-98
WO 99/56429/A1 (Scott)	26-Apr-99	4-Nov-99
C. Adams, "Internet X.509 Public Key Infrastructure Certificate Management Protocols"	n/a	March 1999

A. Hansen, "Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust"	n/a	September 1999
Morton H. Lewin, "A Survey of Read-Only Memories"	n/a	1965
Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication"	n/a	2003
A. Rubin, "Nonmonotonic Cryptographic Protocols"	n/a	1994
P.J. Skevington, "Trusted third parties in electronic commerce"	n/a	April 1997
J.C. Spender, "Identifying Computer Users with Authentication Devices"	n/a	1987
D. Spinellis, "Trusted Third Party Services for Deploying Secure Telemedical Applications over the WWW"	n/a	1999
A. Menezes, Handbook of Applied Cryptography	n/a	1996
Federal Financial Institutions Examination Council, "Authentication in an Electronic Banking Environment" ("FFIEC")	n/a	August 2001
Whitfield Diffie and Martin Hellman, "New Directions in Cryptograph," IEEE Transactions on Information Theory		1976
Nijssen, G.M., <i>Modelling in Data Base Management Systems</i>		1976
Ronald Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM,		1978
Federal Information Processing Standard (FIPS) Publication 46, The Data Encryption Standard (DES)		1977
CCITT, "Series X: Data Communication Networks: The Directory – Authentication Framework"		Nov. 1988

Google additionally identifies and relies on patent or publication references that describe or are otherwise related to the prior art systems identified below. Google's investigation into prior art patent and publication references is ongoing, and Google reserves the right to identify and rely on additional patent or publication references that are identified through further investigation or

discovery. Google reserves the right to supplement as further prior art is identified through investigation or discovery.

2. Prior Art Systems and Products

Google also contends that the Asserted Claims of the '730 Patent, the '954 Patent, and the '905 Patent are invalid based on public knowledge and uses and/or offers for sale or sales of products and services that are prior art under 35 U.S.C. § 102(a) and/or (b); and/or prior inventions made in the United States by other inventors who had not abandoned, suppressed, or concealed them under 35 U.S.C. § 102(g), and that anticipate or render obvious under 35 U.S.C. § 103 the Asserted Claims.

For example, systems and products developed by encryption and/or security concerned companies such as IBM, American Express, HID, and Pocket Vault may constitute prior art:

Prior Art
iCLASS RWKLB575 bioCLASS Biometric Keypad Smart card Reader ("RWKLB575")
Pocket Vault System ("Pocket Vault")
IBM's Secure PDA --CDL Paron MPC ("IBM")
Pay By Touch System ("Pay By Touch")
Bewater FP4000 and FP5000 ("Bewater")
ACS AET65 ("AET65")
Authentic Fingerprint Reader ("Authentec")
DigitalPersona U.are.U for Active Directory ("DigitalPersona")
Connecticut Department of Social Services DSS Digital Imaging Project ("DSS")
Fujitsu DoCoMo FOMA F900i Series ("F900iC")
Identix BioTouch ("BioTouch")
Microsoft Fingerprint Reader
Microsoft Optical Desktop
Microsoft Wireless IntelliMouse
Ringdale Access Control Systems ("Ringdale")
Solus ID08
Sony Puppy Fingerprint Identity Device ("Sony FIU")
Technoimagia FpVTE2003 ("Technoimagia")
UPEK TouchChip Trusted Fingerprint Module ("UPEK")
NTT DoCoMo F505i

Identix IBIS
LAKS MasterCard PayPass Watch
Singtel Mobile Payment
SK Telecom USIM Credit Card
Technoimagia
Ethentica TactileSense
Fujitsu Biometric Mouse

Google is currently in the process of conducting third-party discovery from companies and sources that may have relevant prior art or evidence related to relevant prior art. Google reserves the right to conduct such discovery and supplement its invalidity contentions to include any prior art systems and products that render the asserted claims invalid and/or any evidence that otherwise supports Google's invalidity contentions. Google may use physical samples, executable software, or source code as evidence of the relevant functionality of these prior art products or services. Google will make available for inspection any physical samples of products, systems, or software listed above, and/or any source code therefor, that it has in its possession or that becomes available in the future during discovery.

B. '042/'289/'960 Patents (Hybrid Device Patents)

1. Prior Art Patents and Publications

Prior Art Reference	Effective Filing Date	Publication Date
CA 2,335,532,A1 (De Schrijver)	26-Jun-99	6-Jan-00
CA 2,466,734,A1 (Samar)	22-Jan-03	31-Jul-03
EP 1,224,518,B1 (Vamvakas)	6-Oct-00	15-Jul-09
EP 1,470,534,B1 (Samar)	22-Jan-03	27-Oct-04
EP 1,536,306,A1 ('306 Buer)	30-Sep-04	1-Jun-05
EP 1,864,467,B1 (Vesikivi)	27-Mar-06	12-Dec-07
EP 1,959,369,A1 (Takashi)	10-Dec-99	20-Aug-08
EP 2,797,020,A2(Buer)	30-Sep-04	29-Oct-14
EP 2,797,020,A3(Buer)	30-Sep-04	3-Sep-14
EP 2,937,805,A1 (Buer)	30-Sep-04	28-Oct-15
EP 3,023,899,A1 (Buer)	30-Sep-04	25-May-06
EP 3,023,899,B1 (Buer)	30-Sep-04	16-Sep-20
GB 2,353,386,A (Scott)	26-Apr-99	4-Nov-99
GB 2,353,386,B (Scott)	26-Apr-99	4-Nov-99
GB 2,401,462,A(Chen)	22-Apr-04	10-Nov-04

US 2001/0000535/A1 (Lapsley)	6-Dec-00	26-Apr-01
US 2001/0026632/A1(Tamai)	19-Mar-01	4-Oct-01
US 2001/0030644/A1(Allport)	5-Jun-01	18-Oct-01
US 2002/0003892/A1(Iwanaga)	9-Jul-01	10-Jan-02
US 2002/0046336/A1 (Kon)	30-Aug-01	18-Apr-02
US 2002/0099665/A1(Burger)	1-Oct-01	25-Jul-02
US 2002/0109580/A1 (Shreve)	13-Feb-01	15-Aug-02
US 2002/0116508/A1(Khan)	20-Feb-02	22-Aug-02
US 2002/0126780/A1(Oshima)	5-Dec-01	12-Sep-02
US 2002/0188574/A1 (Niwa)	29-Jul-02	12-Dec-02
US 2002/0194128/A1 (Maritzen)	27-Mar-02	19-Dec-02
US 2003/0037264/A1 (Ezaki)	13-Aug-02	20-Feb-03
US 2003/0051138/A1 (Maeda)	24-Jun-02	13-Mar-03
US 2003/0055792/A1 (Kinoshita)	23-Jul-01	20-Mar-03
US 2003/0074317/A1 (Hofi)	15-Oct-01	17-Apr-03
US 2003/0093693/A1 (Blight)	12-Nov-03	15-May-03
US 2003/0120934/A1 (Ortiz)	10-Jan-01	7-Sep-10
US 2003/0131114/A1 (Scheidt)	15-Oct-02	10-Jul-03
US 2003/0135740/A1 (Talmor)	5-Sep-01	17-Jul-03
US 2003/0140233/A1 (Samar)	22-Jan-02	24-Jul-03
US 2003/0154382/A1 (Vicard)	17-Jan-03	14-Aug-03
US 2003/0177102/A1 (Robinson)	21-Sep-01	18-Sep-03
US 2003/0196084/A1 (Okereke)	11-Apr-03	16-Oct-03
US 2003/0200446/A1 (Siegel)	19-Apr-02	23-Oct-03
US 2003/0220876/A1 (Burger)	19-Mar-03	27-Nov-03
US 2004/0014423/A1 (Croome)	14-May-03	22-Jan-04
US 2004/0044627/A1 (Russell)	29-Nov-00	4-Mar-04
US 2004/0123106/A1 (D'Angelo)	26-Aug-03	24-Jun-04
US 2004/0148526/A1 (Sands)	24-Jan-03	29-Jul-04
US 2004/0153649/A1 (Rhoads)	27-Jul-95	3-Aug-10
US 2004/0255139/A1 (Giobbi)	27-Dec-00	4-Dec-07
US 2004/0257196/A1 (Kotzin)	20-Jun-03	23-Dec-04
US 2005/0005136/A1(Chen)	21-Apr-04	6-Jan-05
US 2005/0039027/A1 (Shapiro)	25-Jul-03	17-Feb-05
US 2005/0091213/A1 (Schutz)	23-Oct-03	28-Apr-05
US 2005/0105734/A1 (Buer)	30-Sep-04	19-May-05
US 2005/0218215/A1 (Lauden)	31-Mar-05	6-Oct-05
US 2005/0221798/A1 (Sengupta)	30-Mar-04	6-Oct-05
US 2005/0225430/A1 (Seifert)	19-Dec-02	13-Oct-05
US 2005/0253683/A1 (Lowe)	17-May-04	17-Nov-05
US 2005/0269401/A1 (Spitzer)	3-Jun-05	8-Dec-05
US 2005/0273440/A1 (Ching)	13-May-05	8-Dec-05
US 2006/0080525/A1 (Ritter)	11-Oct-05	13-Apr-06
US 2006/0081714/A1 (King)	23-Aug-05	20-Apr-06
US 2006/0129838/A1 (Chen)	8-Aug-02	15-Jun-06

US 2006/0136717/A1 (Buer)	15-Aug-05	22-Jun-06
US 2006/0136741/A1 (Mercredi)	16-Dec-04	22-Jun-06
US 2006/0142058/A1 (Elias)	17-Feb-06	29-Jun-06
US 2006/0204048/A1 (Morrison)	25-Mar-05	14-Sep-06
US 2006/0248554/A1 (Priddy)	27-Jun-06	2-Nov-06
US 2007/0038867/A1 (Verbauwhede)	2-Jun-04	15-Feb-07
US 2007/0057763/A1 (Blattner)	12-Sep-05	15-Mar-07
US 2007/0156436/A1 (Fisher)	25-Aug-06	5-Jul-07
US 2007/0245157/A1 (Giobbi)	7-May-07	18-Oct-07
US 2007/0245158/A1 (Giobbi)	7-May-07	18-Oct-07
US 2007/0260883/A1 (Giobbi)	5-May-07	8-Nov-07
US 2008/0100414/A1 (Diab)	30-Oct-06	1-May-08
US 2008/0100414/A2 (Diab)	30-Oct-06	13-Mar-13
US 2008/0150678/A1 (Giobbi)	13-Nov-07	26-Jun-08
US 2009/0094681/A1 (Sadler)	3-Oct-07	9-Apr-09
US 2009/0215385/A1 (Waters)	15-Feb-05	27-Aug-09
US 2010/0049987/A1 (Ettorre)	19-Dec-06	25-Feb-10
US 2010/0062743/A1 (Jonsson)	20-Aug-04	11-Mar-10
US 5,708,422 (Blonder)	31-May-1995	13-Jan-1998
US 5,623,552,A (Lane)	15-Aug-94	22-Apr-97
US 5,867,795,A (Novis)	23-Aug-96	2-Feb-99
US 6,011,858,A (Stock)	10-May-96	4-Jan-00
US 6,016,476,A (Maes)	16-Jan-98	18-Jan-00
US 6,104,922,A (Baumann)	2-Mar-98	15-Aug-00
US 6,219,439,B1 (Burger)	9-Jul-98	17-Apr-01
US 6,325,285,B1 (Baratelli)	12-Nov-99	4-Dec-01
US 6,353,889,B1 (Hollingshead)	13-May-98	5-Mar-02
US 6,751,734,B1 (Uchida)	21-Mar-00	15-Jun-04
US 6,819,219,B1 (Bolle)	12-Oct-00	16-Nov-04
US 6,907,135,B2 (Gifford)	2-Mar-99	14-Jun-05
US 6,957,339,B2 (Shinzaki)	7-Jun-02	18-Oct-05
US 7,155,416,B2 (Shatford)	3-Jul-03	26-Dec-06
US 7,174,031,B2 (Rhoads)	17-May-05	6-Feb-07
US 7,188,110,B1 (Ludtke)	11-Dec-00	6-Mar-07
US 7,200,755,B2 (Hamid)	24-May-01	3-Apr-07
US 7,249,112,B2 (Berardi)	13-Dec-02	24-Jul-07
US 7,310,042,B2 (Seifert)	19-Dec-04	18-Dec-07
US 7,404,086,B2 (Sands)	24-Jan-03	22-Jul-08
US 7,478,065,B2 (Ritter)	23-Dec-99	13-Jan-09
US 7,561,691,B2 (Blight)	12-Nov-01	14-Jul-09
US 7,636,854,B2 (Müller)	2-May-02	22-Dec-09
US 7,690,577,B2 (Beenau)	20-Sep-07	6-Apr-10
US 7,694,331,B2 (Vesikivi)	1-Apr-05	6-Apr-10
US 8,166,523,B2 (Ezaki)	13-Aug-02	24-Apr-12
US 8,200,980,B1 (Robinson)	7-Jun-04	12-Jun-12

US 8,232,862,B2 (Lowe)	17-May-04	31-Jul-12
US 8,249,935,B2 (DiMartino)	27-Sep-07	21-Aug-12
US 8,333,317,B2 (Buer)	30-Sep-04	18-Dec-12
US 8,395,478,B2 (Diab)	30-Oct-06	12-Mar-13
US 8,548,927,B2 (Beenau)	10-Jul-01	1-Oct-13
US 8,594,563,B2 (Waters)	15-Feb-05	26-Nov-13
US 8,893,284,B2 (Sadler)	3-Oct-07	18-Nov-14
US 8,955,083,B2 (Ettorre)	19-Dec-06	10-Feb-15
US 9,042,819,B2 (Dua)	12-May-05	15-Jan-15
US 9,269,221,B2 (Gobbi)	13-Nov-07	23-Feb-16
US 9,542,542,B2 (Giobbi)	7-May-07	10-Jan-17
WO 00/00882/A2 (De Schrijver)	25-Jun-99	6-Jan-00
WO 00/00923/A1 (Valliani)	30-Jun-99	6-Jan-00
WO 01/027723/A1 (Vamvakas)	6-Oct-00	19-Apr-01
WO 01/27723/A1 (Vamvakas)	6-Oct-00	19-Apr-01
WO 02/089018/A1 (Pu)	2-May-01	7-Nov-02
WO 02/095547/A2 (Hamid)	23-Apr-02	28-Nov-02
WO 03/003295/A1 (Poo)	28-Jun-01	9-Jan-03
WO 03/036861/A1 (Black)	28-May-02	1-May-03
WO 03/054806/A2 (Seifert)	19-Dec-02	3-Jul-03
WO 03/063094/A2 (Samar)	22-Jan-02	31-Jul-03
WO 03/093923/A2 (Eryou)	30-Apr-03	13-Nov-03
WO 2004/019190/A1 (Chen)	8-Aug-02	4-Mar-04
WO 2004/068283/A2 (Sands)	23-Jan-04	12-Aug-04
WO 2007/0198436/A1 (Weiss)	21-Feb-07	23-Aug-07
WO 2007/133541/A2 (Giobbi)	7-May-07	22-Nov-07
WO 2008/0022089/A1 (Leedom)	26-Jun-06	24-Jan-08
WO 90/006633/A1 (Lee)	9-Dec-98	14-Jun-90
WO 98/12670/A1 (Borza)	15-Sep-97	26-Mar-98
WO 99/56429/A1 (Scott)	26-Apr-99	4-Nov-99
Iftode et. al, "Smart Phone: An Embedded System for Universal Interactions"	n/a	2006
European Parliament Scientific Technology Options Assessment, "RFID and Identity Management in Everyday Life"	n/a	2006
Hwang, "Wireless Access Monitoring and Control System based on Digital Door Lock"	n/a	2007
Shillingford, "Mobile wallets start to take shape," BBC News business reporter	n/a	March 1, 2005
Zmijewska, "Evaluating Wireless Technologies in Mobile Payments – A Customer Centric Approach"	n/a	2005

2. Prior Art Systems and Products

Google also contends that the Asserted Claims of the '042 Patent, the '289 Patent, and the '960 Patent are invalid based on public knowledge and uses and/or offers for sale or sales of products and services that are prior art under 35 U.S.C. § 102(a) and/or (b); and/or prior inventions made in the United States by other inventors who had not abandoned, suppressed, or concealed them under 35 U.S.C. § 102(g), and that anticipate or render obvious under 35 U.S.C. § 103 the Asserted Claims.

For example, systems and products developed by encryption and/or security concerned companies such as Broadcom, HID, and Pocket Vault may constitute prior art:

Prior Art
Broadcom Proximity Authentication System ("Broadcom")
iCLASS RWKLB575 bioCLASS Biometric Keypad Smart card Reader ("RWKLB575")
Pocket Vault System ("Pocket Vault")
Authentec Fingerprint Reader ("Authentec")
DigitalPersona U.are.U for Active Directory ("DigitalPersona")
HTC phones with Bluetooth, NFC, IrDA, or Wi-Fi communication capabilities, including Blue Angel, Magician, Canary, Vox, and Touch
Identix BioTouch ("BioTouch")
Microsoft Fingerprint Reader
Microsoft Optical Desktop
Microsoft Wireless IntelliMouse
Ringdale Access Control Systems ("Ringdale")
Solus ID08
Sony-Ericsson phones with Bluetooth, NFC, IrDA, or Wi-Fi communication capabilities, including K550, W550, P910, and S500
Sony Puppy Fingerprint Identity Device ("Sony FIU")
Technomagia FpVTE2003 ("Technomagia")
UPEK TouchChip Trusted Fingerprint Module ("UPEK")
NTT DoCoMo F505i
Identix IBIS
LAKS MasterCard PayPass Watch
Singtel Mobile Payment
SK Telecom USIM Credit Card
Technomagia

Nokia phones with Bluetooth, NFC, IrDA, or Wi-Fi communication capabilities, including N95, N77, 6131, 6131 NFC, 6136, and 5300
Toyota Remote Engine Starter
ETSI – the SIM

Google is currently in the process of conducting third-party discovery from companies and sources that may have relevant prior art or evidence related to relevant prior art. Google reserves the right to conduct such discovery and supplement its invalidity contentions to include any prior art systems and products that render the asserted claims invalid and/or any evidence that otherwise supports Google’s invalidity contentions. Google may use physical samples, executable software, or source code as evidence of the relevant functionality of these prior art products or services. Google will make available for inspection any physical samples of products, systems, or software listed above, and/or any source code therefor, that it has in its possession or that becomes available in the future during discovery.

VI. INVALIDITY UNDER 35 U.S.C. §102 AND §103

A. ’730/’954/’905 Patents (Device ID Patents)

At this time, Google contends that at least each of the prior art references described and charted in Exhibits 730-01-43 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the ’730 patent.

Likewise, Google contends that at least each of the prior art references described and charted in Exhibits 954-01-44 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the ’954 Patent.

Likewise, Google contends that at least each of the prior art references described and charted in Exhibits 905-01-44 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the ’905 Patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the Asserted Patents, including without limitation as evidence of the state of the art at the alleged time of invention (*see also* Section IV.A), has been included in Google's production of prior art. Google reserves the right to amend these invalidity contentions to assert these references depending on the infringement positions Proxense may take as the case proceeds and Google's ongoing investigation. Moreover, Google reserves the right to use these references in combination with other references to render the claims of the '730 Patent, the '954 Patent, and the '905 Patent obvious in the event Proxense takes the position that certain claim limitations are missing from the references charted in Exhibits 730-01-43, 954-01-44, and 905-01-44.

1. Anticipation

Google contends that the Asserted Claims of the '730 Patent, the '954 Patent, and the '905 Patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references in Exhibits 730-01-43, 954-01-44, and 905-01-44, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. The cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claims of the '730 Patent, the '954 Patent, or the '905 Patent, Google reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of ordinary skill in the art, even if Google has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

2. Obviousness

Each anticipatory prior art reference disclosed in the preceding section, either alone or in combination with other prior art, also renders the Asserted Claims of the Asserted Patents invalid as obvious, and as demonstrated in the claim charts appended as Exhibits 730-01-43, 954-01-44, and 905-01-44. To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in Exhibits 730-01-43, 954-01-44, and 905-01-44, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more asserted claims of the Asserted Claims obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. To the extent any of the references in Exhibits 730-01-43, 954-01-44, and 905-01-44 is deemed to lack a particular claim limitation, that reference can be combined with the disclosure identified for that limitation in Exhibits 730-B, 954-B, and 905-B to render that limitation and Proxense's claims a whole obvious. Google may also show that such an allegedly lacking limitation is rendered obvious by the disclosure of any of the other references identified in Exhibits 730-01-43, 954-01-44, and 905-01-44.

Google also reserves the right to amend or supplement these contentions regarding anticipation or the obviousness of the Asserted Claims in view of further information from Proxense, or information discovered during discovery. Proxense has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore,

for any claim limitation that Proxense alleges is not disclosed in a particular prior art reference, Google reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the asserted claim obvious.

3. Motivation to Combine

Google intends to present expert evidence demonstrating the motivation to combine of one of ordinary skill in the art. Such facts and evidence is expert testimony and will be presented in the experts' reports according to the schedule of the Court. Google incorporates by reference its forthcoming expert reports and any testimony of its experts presented according to the Court's schedule. The motivation to combine or modify the above items of prior art are present, for example, in the references themselves, the Patents-in-Suit, references cited on the face of the Patents-in-Suit, the knowledge, skill, or creativity of one of ordinary skill in the art, the prior art as a whole, and/or the nature of the problems allegedly addressed by the Patents-in-Suit. The law requires no showing of a specific motivation to combine or modify prior art references disclosed herein and in the Invalidity Charts, as each combination or modification of art would have no unexpected results and at most would simply represent a known alternative to one of skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 127 S.Ct. 1727, 1739-40 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test, instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases, a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 1742. Thus, to a person of ordinary skill in the art, the Asserted Claims represent solutions that would have been obvious to try, with predictable results.

Nevertheless, should additional evidence of motivation to combine or modify be required to render the Asserted Claims obvious, Google contends that there was a motivation to combine the references identified above. That motivation was provided in the nature of the problem allegedly solved by the Patents-in-Suit, the teachings of the cited prior art itself, and/or the knowledge of a person of ordinary skill in the art. For example, the combinations identified above would have been combined or modified using: known methods to yield predictable results; common sense; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or a teaching, suggestion, or motivation in the prior art generally. In addition, it would have been obvious to try combining or modifying the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field of endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. In addition, the combination of the prior art references would have been obvious because the combination represents known potential options with a reasonable expectation of success. Specific examples of such motivations to combine are outlined below, and are not meant to be exhaustive.

Additional evidence that there would have been a motivation to combine or modify the prior art references above includes the interrelated teachings of multiple prior art references; the effects of demands known to the design community or present in the marketplace; the existence of a known problem for which there was an obvious solution encompassed by the Asserted Claims; the existence of a known need or problem in the field of the endeavor at the time of the alleged invention(s); and the background knowledge, skill, or creativity that would have been possessed by a person having ordinary skill in the art. Google may rely on uncited portions of the prior art references cited and produced, other publications and testimony, and the testimony of experts to

establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious. For example, where multiple publications describe the same system, multiple devices intended to be used together, or are from the same author or publisher, one of ordinary skill would be motivated and find it obvious to read those publications together and combine their disclosure. As another example, where a product was available in another country, the availability of such a product would motivate a person of ordinary skill to arrive at the same or similar product in the United States. As yet another example, where the prior art identifies the desirability of or plans for future enhancements of a system, a person of ordinary skill would be motivated to incorporate such enhancements even if the original developer or author was unable to complete those enhancements for business reasons.

References identified by Google address the same technical issues and suggest very similar solutions to those issues discussed in the Patents-in-Suit and generally known at the time of the alleged invention(s) claimed in the Asserted Claims. Google reserves the right to supplement these Invalidity Contentions with additional charts for any of the references listed in above, and/or common knowledge and state of the art.

Each of the references cited above is in the encryption or security space and would have been known to a person of ordinary skill in the art. In addition, the types of access described in the cited references, e.g., to financial information, to perform a financial transaction, or physical access to a location or room, were examples of situations requiring security well-known to a person of ordinary skill in the art. Further, because each of the cited references are also directed to authenticating a user using biometrics on a device in order to grant access to function, service or application, a person of skill in the art would have been motivated to combine those references.

For example, Google incorporates by reference all motivations to combine referenced in all *inter partes* review and *ex parte* reexamination requests filed challenging the Asserted Patents and any related patents. See, e.g., IPR2021-01444; IPR2021-01447; IPR2021-01448; IPR2024-00232; IPR2024-00233; IPR2024-00234; Reexamination Nos. 90/015,052, 90/015,053, 90/015,054. As another example, one of ordinary skill in the art would have been motivated to combine Burger with Scott because Burger specifically identifies Identix, which is the assignee of the Scott reference. See Burger at [0135]. As another example, a POSA would have been motivated to combine Stock with Scott because Stock specifically identifies Identix. See Stock at 5:55-65. One of ordinary skill in the art would have been familiar with the major developers and equipment providers in the security space. As Burger and Stock specifically note, one of ordinary skill would expect to use components from a variety of companies in this space. This is similarly true of the underlying technologies embodied by the above noted references. For example, Russell specifically mentions Stock at ¶25. Likewise, one of ordinary skill would recognize many of the commonly approached problems. For example, Ludtke, Pocket Vault, Burger, Lapsley, Hofi, Scott, and Berardi all relate to authenticating and authorizing financial transactions. Moreover, these references also use similar two-factor biometric and device authentication. Other references such as Burger, RWKLB575, Pocket Vault, and Scott relate to authenticating a user using similar two-factor authentication mechanisms to enable physical access to a location. One of ordinary skill in the art would look to references that address similar problems (need to authenticate) with similar means to solve that problem (two-factor authentication methods). As such one of ordinary skill in the art would be motivated to combine these references.

Indeed, by the alleged priority date of the Device ID patents, biometric authentication to protect access to cell phones was well known, including cell phones with mobile wallet

applications installed thereon that could be used as replacements for credit cards – the very technology now accused of infringement by Proxense. See Exhibits 730-34, 905-34, and 954-34. Such commercial use of the claimed technology, in addition to qualifying as anticipatory and obviousness prior art in its own right, would have further motivated a POSITA to arrive at the asserted claims and have a reasonable expectation of success in doing so.

As discussed above in Section IV.A, the '730 Patent, the '954 Patent, and the '905 Patent purport to address challenges in requiring users to “memorize or otherwise keep track of the[ir] credentials” and illegitimate users “us[ing] a stolen access object to enter a secured location because the user’s identity is never checked.” ’730 Patent at 1:23-48. Both of these were well-known problems with well-known solutions. For example, the general principle of multi-factor security had been well-established in the industry prior to the year 2000. As detailed below and in Google’s invalidity charts, to the extent that any of the claimed components are not inherent in an authentication system, a person of ordinary skill in the art would have been motivated to add them as one of a limited number of design options available when implementing a method of secure access control. For example, in his 1999 dissertation, Hansen describes the classical taxonomy of authentication methods (something the user has, something the user knows, or something the user is), and explains that “most practical systems combine elements to improve security.” Hansen at 15. Thus, the weaknesses of these individual authentication methods were well-known at the time. In a 2003 essay, O’Gorman breaks down the limitations of each of these authentication methods. O’Gorman at 2037. For example, O’Gorman writes that using passwords, or something a user knows, presents the problem that “humans have difficulty remembering” them and that “they do not provide good compromise detection, and they do not offer much defense against repudiation.” *Id.* Tokens, or something the user has, present the

disadvantages of “inconvenience and cost,” where “[e]quipment cost is higher than a password, but comparable to a biometric that requires a reader.” *Id.* Using biometrics, or something the user is, presents the potential downside that “the recognition rate for speaker verification may not be high enough to provide security without inconveniencing the user by many false nonmatches.” *Id.* Addressing these vulnerabilities, O’Gorman acknowledges that “[t]he system is only as good as its weakest defense, and multiple lines of defense are better than one.” *Id.* Thus, in any authentication scheme, it was generally well-known and obvious to combine multiple forms of authentication in order to increase security.

Additional motivation to incorporate any of the concepts claimed in the ’730 Patent, the ’954 Patent, and the ’905 Patent into any primary reference allegedly missing those concepts is set forth below:

a. Biometric Authentication

As discussed above in Section IV.A.1 (incorporated herein by reference), the ’730 Patent, the ’954 Patent, and the ’905 Patent claim the use of biometric verification. As addressed in the “Background” section above and the accompanying claim charts, use of biometric authentication was well known in the art and frequently combined with other authentication methods, including in an ever growing number of consumer products. *See also* <https://apps.dtic.mil/sti/tr/pdf/ADA318942.pdf>. Thus, a POSITA would have recognized this market trend towards and documented benefit of integrating biometric verification into an authentication scheme and been motivated to incorporate the same into other products and systems.

Moreover, incorporating biometric verification into an authentication scheme would also achieve known benefits of allowing stronger user authentication (harder to copy a fingerprint than steal a token or crack a password), avoiding need to memorize passwords, and combining

multiple authentication methods to improve security (similar to the use of a credit card in combination with a PIN to access an ATM).

Finally, a POSITA would have had a reasonable expectation of success, including as evidenced by the fact that biometric authentication was already being incorporated into various consumer products before the priority date of the Device ID patents.

b. Device IDs

As discussed above in Section IV.A.2 (incorporated herein by reference), the '730 Patent, the '954 Patent, and the '905 Patent claim the use of a device ID that “uniquely identif[ies] the integrated device.” As addressed in the “Background” section above and the accompanying claim charts, use of such device identifiers for authentication was well known in the art and frequently combined with other authentication methods, including in an ever growing number of consumer products. Thus, a POSITA would have recognized this market trend towards and documented benefit of using a device ID as part of an authentication scheme and been motivated to incorporate the same into other products and systems.

Moreover, using a device ID in an authentication scheme would also achieve known benefits of allowing stronger user authentication (by assigning a unique identifier to a device used to specifically identify that device), avoiding need to memorize passwords, and combining multiple authentication methods to improve security (similar to the use of a credit card with a unique number in combination with a PIN to access an ATM).

Indeed, as the patent examiner determined in the March 4, 2024 Final Rejection during *ex parte* reexamination of the '905 patent, prior art Okereke “specifically teaches transmission of a device’s unique identifier to a proxy as part of a scheme to authenticate the device,” and “it would have been obvious to one of ordinary skill at the time of the invention to have employed the techniques of Okereke with that of Ludke in order to facilitate secure communications

between the elements of Ludtke, including transmission of a transaction device's stored unique identifier." *Ex parte* reexamination of U.S. Patent 9,298,905, Control No. 90/015,063, March 4, 2024 Final Rejection at 5. According to the examiner, "[o]ne of ordinary skill would have expected this to yield a predictable result of providing security through encryption with a private key, as well as the ability to ensure authentication of an authorized device using unique." *Id.* at 5-6.

Finally, a POSITA would have had a reasonable expectation of success, including as evidenced by the fact that various consumer products and standardized technologies used device identifiers before the priority date of the Device ID patents.

c. Memory That Cannot Be Altered / Temper Proof

As discussed above in Section IV.A.3 (incorporated herein by reference), the '730 Patent, the '954 Patent, and the '905 Patent claim the use of "persistent storage," "a tamper proof format," and/or "a storage element ... is unable to be subsequently altered."

As addressed in the "Background" section above and the accompanying claim charts, use of "tamper proof" memory or a "storage element [that] is unable to be subsequently altered" was well known in the art and frequently combined with other security mechanisms, including in an ever growing number of consumer products. Thus, a POSITA would have recognized this market trend towards and documented benefit of using such memory to store sensitive data (including biometric information, device ID, and other data that may allow a bad actor to gain unpermitted access) and been motivated to incorporate the same into other products and systems.

Moreover, using a tamper-proof format and/or memory that cannot be subsequently altered would also achieve known benefits in data security. Particularly in authentication schemes that incorporate the use of sensitive personal information, such as biometric data, it would have been obvious for a POSITA to implement read-only memory in order to better store

and protect such data and mitigate the risk of stealing credentials. Additionally, a POSITA would have been motivated to incorporate read-only memory into existing authentication schemes in order to prevent the security threat of injecting false or unverified credentials. For example, the alleged benefits of using biometric verification would be quickly negated if a bad actor were able to either (1) alter the biometric data on a stolen device to reflect the bad actor's biometrics; or (2) alter the device ID on a legitimately purchased device to reflect an intercepted or otherwise stolen device ID code. In either scenario, the bad actor would be able to mimic a real user and gain unauthorized access to applications, financial accounts, etc.

Finally, a POSITA would have had a reasonable expectation of success, including as evidenced by the fact that various consumer products and standardized technologies used temper proof formatting and/or memory that cannot be subsequently altered even before the priority date of the Device ID patents. Indeed, the Device ID patents do not purport to invent any new technical solution to temper proof formatting or securing memory, and instead simply reference such technology as if it was well known even before their priority date (which it was). '730 patent at 4:29-42. Existing read-only memory drives had existed on the market for decades, and had been successfully implemented in a multitude of access control applications.

d. Third-Party Trusted Authority

As discussed above in Section IV.A.4 (incorporated herein by reference), all asserted claims of the Device ID patents require a "trusted third party authority."

As addressed in the "Background" section above and the accompanying claim charts, use of "trusted third party authorities" for authentication was well known in the art and frequently combined with other security mechanisms, including in an ever growing number of consumer products. Indeed, we use third party authorities all the time in less technical contexts (impartial jury deciding a dispute, public notary verifying identity of parties signing contracts, escrow

agency holding money during, e.g., a house purchase). The same is true in technical contexts. For example, security on the Internet relies largely on SSL/TSL, which in turn is based on certificate authorities acting as third party trusted authorities. More generally, the entire field of public key infrastructure depends on the presence of trusted third parties and public-key certificates. Thus, a POSITA would have recognized this market trend towards and documented benefit of using such third party trusted authorities (including having an arbitrator to a transaction) and been motivated to incorporate the same into other products and systems.

Moreover, using a third party trusted authority would also achieve known benefits in data security. Having a third party trusted authority track and verify user credentials prevents other parties to a transaction (including for example vendors on the Internet) from having direct access to a multitude of sensitive user credentials. Having fewer entities with access to this kind of information makes it less likely for a bad actor to gain access to this information by, for example, pretending to be a legitimate vendor. In addition, a third party trusted authority is better positioned to deploy a specialized, highly secure, data network and associated database than individual vendors who do not specialize in maintaining sensitive data.

Finally, a POSITA would have had a reasonable expectation of success, including as evidenced by the fact that various consumer products and standardized technologies use and/or rely on third-party trusted authorities.

e. Access Message

As discussed above in Section IV.A.5 (incorporated herein by reference), the '730 Patent, the '954 Patent, and the '905 Patent claim the use of “access message from the agent allowing the user access to an application” or “complete a financial transaction.”

As addressed in the “Background” section above and the accompanying claim charts, use of “access messages” in connection with authentication was well known in the art and frequently

combined with other security mechanisms, including in an ever growing number of consumer products. Indeed, once a user is authenticated in such a system, the natural next step is to allow access to whatever prompted the authentication process in the first instance, and the obvious way to do that is via an access message. Thus, a POSITA would have recognized this market trend towards and documented benefit of using such access messages (including as a necessity to allowing access) and been motivated to incorporate the same into other products and systems.

Moreover, using an access message would also achieve known benefits in data security. Particularly in security applications where a third party trusted authority is involved, the concept of providing an “access message” would have been obvious to implement, as some communication would be necessary between the third-party trusted authority and host system once verification is confirmed. Moreover, sending an “access message” rather than the information itself advances the advantages of using a third party trusted authority in the first instance, since no sensitive data needs to be revealed to the second party to the transaction, and instead the second party only needs to receive a notification allowing access.

Finally, a POSITA would have had a reasonable expectation of success, including as evidenced by the fact that various consumer products and standardized technologies use and/or rely on access messages.

B. '042/'289/'960 Patents (Hybrid Device Patents)

At this time, Google contends that at least each of the prior art references described and charted in Exhibits 042-01-31 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the '042 Patent.

Likewise, Google contends that at least each of the prior art references described and charted in Exhibits 289-01-31 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the '289 Patent.

Likewise, Google contends that at least each of the prior art references described and charted in Exhibits 960-01-31 anticipates or renders obvious, either alone or in combination, one or more of the asserted claims of the '960 Patent.

Additional prior art that has not been charted, but is still relevant to the invalidity of the Asserted Patents, including without limitation as evidence of the state of the art at the alleged time of invention (*see also* Section IV.A), has been included in Google's production of prior art. Google reserves the right to amend these invalidity contentions to assert these references depending on the infringement positions Proxense may take as the case proceeds and Google's ongoing investigation. Moreover, Google reserves the right to use these references in combination with other references to render the claims of the '042 Patent, the '289 Patent, and the '960 Patent obvious in the event Proxense takes the position that certain claim limitations are missing from the references charted in Exhibits 042-01-31, 289-01-31, and 960-01-31.

1. Anticipation

Google contends that the Asserted Claims of the '042 Patent, the '289 Patent, and the '960 Patent are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references in 042-01-31, 289-01-31, and 960-01-31, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art references. The cited portions of prior art references identified in the attached claim charts are exemplary only and representative of the content and teaching of the prior art references, and should be understood in the context of the reference as a whole and as they would be understood by a person of ordinary skill in the art.

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claims of the '042 Patent, the '289 Patent, and the '960 Patent, Google reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art, or obvious to a person of

ordinary skill in the art, even if Google has not specifically denoted that the art is to be combined with the knowledge of a person of ordinary skill in the art.

2. Obviousness

Each anticipatory prior art reference disclosed in the preceding section, either alone or in combination with other prior art, also renders the Asserted Claims of the Asserted Patents invalid as obvious, alone, and as demonstrated in the claim charts appended as Exhibits 042-01-31, 289-01-31, and 960-01-31. To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in Exhibits 042-01-31, 289-01-31, and 960-01-31, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, the references identified above render one or more asserted claims of the Asserted Claims obvious when the references are read in combination with each other, and/or when read in view of the state of the art and knowledge of those skilled in the art. Each and every reference identified is also relevant to the state of the art at the time of the alleged invention. To the extent any of the references in Exhibits 042-01-310, 289-01-310, and 960-01-31 is deemed to lack a particular claim limitation, that reference can be combined with the disclosure identified for that limitation in Exhibits 042-B, 289-B, and 960-B to render that limitation and Proxense's claims a whole obvious. Google may also show that such an allegedly lacking limitation is rendered obvious by the disclosure of any of the other references identified in Exhibits 042-01-310, 289-01-310, and 960-01-31.

Google also reserves the right to amend or supplement these contentions regarding anticipation or the obviousness of the Asserted Claims in view of further information from

Proxense, or information discovered during discovery. Proxense has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that Proxense alleges is not disclosed in a particular prior art reference, Google reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the asserted claim obvious.

3. Motivation to Combine

Google intends to present expert evidence demonstrating the motivation to combine of one of ordinary skill in the art. Such facts and evidence is expert testimony and will be presented in the experts' reports according to the schedule of the Court. Google incorporates by reference its forthcoming expert reports and any testimony of its experts presented according to the Court's schedule. The motivation to combine or modify the above items of prior art are present, for example, in the references themselves, the Patents-in-Suit, references cited on the face of the Patents-in-Suit, the knowledge, skill, or creativity of one of ordinary skill in the art, the prior art as a whole, and/or the nature of the problems allegedly addressed by the Patents-in-Suit. The law requires no showing of a specific motivation to combine or modify prior art references disclosed herein and in the Invalidity Charts, as each combination or modification of art would have no unexpected results and at most would simply represent a known alternative to one of skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 127 S.Ct. 1727, 1739-40 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test, instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases, a person of ordinary skill in the art will be able to fit the teachings of multiple patents

together like pieces of a puzzle.” *Id.* at 1742. Thus, to a person of ordinary skill in the art, the Asserted Claims represent solutions that would have been obvious to try, with predictable results.

Nevertheless, should additional evidence of motivation to combine or modify be required to render the Asserted Claims obvious, Google contends that there was a motivation to combine the references identified above. That motivation was provided in the nature of the problem allegedly solved by the Patents-in-Suit, the teachings of the cited prior art itself, and/or the knowledge of a person of ordinary skill in the art. For example, the combinations identified above would have been combined or modified using: known methods to yield predictable results; common sense; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or a teaching, suggestion, or motivation in the prior art generally. In addition, it would have been obvious to try combining or modifying the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field of endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. In addition, the combination of the prior art references would have been obvious because the combination represents known potential options with a reasonable expectation of success.

Additional evidence that there would have been a motivation to combine or modify the prior art references above includes the interrelated teachings of multiple prior art references; the effects of demands known to the design community or present in the marketplace; the existence of a known problem for which there was an obvious solution encompassed by the Asserted Claims; the existence of a known need or problem in the field of the endeavor at the time of the alleged invention(s); and the background knowledge, skill, or creativity that would have been possessed by a person having ordinary skill in the art. Google may rely on uncited portions of the prior art

references cited and produced, other publications and testimony, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious. For example, where multiple publications describe the same system, multiple devices intended to be used together, or are from the same author or publisher, one of ordinary skill would be motivated and find it obvious to read those publication together and combine their disclosure. As another example, where a product was available in another country, the availability of such a product would motivate a person of ordinary skill to arrive at the same or similar product in the United States. As yet another example, where the prior art identifies the desirability of or plans for future enhancements of a system, a person of ordinary would be motivated to incorporate such enhancements even if the original developer or author was unable to complete those enhancements for business reasons.

References identified by Google address the same technical issues and suggest very similar solutions to those issues discussed in the Patents-in-Suit and generally known at the time of the alleged invention(s) claimed in the Asserted Claims. Google reserves the right to supplement these Invalidity Contentions with additional charts for any of the references listed in above, and/or common knowledge and state of the art.

Each of the references cited above is in the encryption or security space and would have been known to a person of ordinary skill in the art. In addition, the types of access described in the cited references, e.g., to financial information, to perform a financial transaction, or physical access to a location or room, were examples of situations requiring security well-known to a person of ordinary skill in the art. Further, because each of the cited references are also directed to authenticating a user using biometrics on a device in order to grant access to function, service or application, a person of skill in the art would have been motivated to combine those references.

For example, Google incorporates by reference all motivations to combine referenced in all *inter partes* review and *ex parte* reexamination requests filed challenging the Asserted Patents and any related patents. *See, e.g.*, IPR2021-01438; IPR2021-01439; IPR2024-00405; IPR2024-00407; IPR2024-00573. As another example, one of ordinary skill in the art would have been motivated to combine Buer I and Leedom because both references describe encryption and authentication methods to be implemented on personal devices such as personal data assistants (“PDA”) and cell phones. *See* Buer I at [0163], Leedom at [0034]. As another example, it would have been obvious for a POSITA to combine Giobbi ‘157 with Leedom for the same reason – Giobbi ‘157 also describes authentication methods that can be implemented into cell phones and Personal Digital Assistants. *See* Giobbi ‘157 at [0035]. Further, other references such as RWKLB575 and Pocket Vault relate to authenticating a user using similar two-factor authentication mechanisms to enable physical access to a location. *See* Exs. 042-13-14, 289-13-14, 960-13-14. One of ordinary skill in the art would look to references that address similar problems (need for encryption/authentication on PDAs and cell phones) with similar means to solve that problem. As such one of ordinary skill in the art would be motivated to combine these references.

As another example, a POSITA would be specifically motivated to combine Dua with Giobbi ‘139 and Giobbi ‘157 references to arrive at the claims of the Hybrid Patents. Dua further corroborates the teachings of the Giobbi references and provides implementation details for integrating an RDC and PDK into the same device. A POSITA would have recognized the similarity between 1) the RFID Tag in Dua and the PDK in Giobbi ‘157; and 2) the RFID Reader in Dua and the RDC in Giobbi ‘139. This is because, like RFID technology, Giobbi’s PDK and RDC architecture require both components within proximity of each other. For example, two

RFID tags without a reader would not be usable. Likewise, two PDKs without an RDC would not be usable. An RFID tag becomes usable when in range of an RFID reader, comparable to how a PDK is usable when in range of an RDC. A POSITA would have been motivated to combine the teachings of the Giobbi references and Dua because, at least, these references are all in the same field of endeavor. Giobbi '157, Abstract, ¶¶[0011]-[0014]; Giobbi '139, Abstract, ¶[0010]; Dua, Abstract, 6:46-65, FIGS. 4A, 6; '042 Patent, Abstract, claim 1. Accordingly, with proximity enabling technology (RFID) like Dua integrating both transmitters (PDKs/RFID Tags) and receivers (RDCs/RFID Readers) into the same mobile device, a POSITA would have had a reasonable expectation of success integrating an RDC from Giobbi '139 into the Giobbi '157 device to create a hybrid device. *Id.* This reasonable expectation of success is further bolstered by the teachings of Dua, which, as discussed above, also teaches integrating an “RDC” and “PDK” into the same type of device. Dua, 13:19-14:64, Fig. 4A. Given the teachings of Giobbi '157 and Giobbi '139, a POSITA would have been motivated to integrate a PDK and RDC into the same mobile device (thus, creating a “hybrid device”). Giobbi '157, ¶¶[0012], [0027], [0030], [0035]; Giobbi '139, ¶¶[0022]-[0044]. Giobbi '157 enumerates the advantages and motivations of incorporating a PDK into a mobile device. Giobbi '157, ¶¶[0035], [0080], claims 27, 33. For example, a user carrying the hybrid device would be able to be wirelessly authenticated with RDCs to securely complete transactions or gain access to physical or digital assets. Each RDC would be capable of communicating with the PDK’s “secure and tamperproof memories,” in which biometric authentication data is stored securely on the device in a format retrievable by an RDC. Giobbi '157, ¶¶[0036], [0064]. Additionally, Giobbi '139 teaches the benefits of integrating an RDC into this hybrid device. Giobbi '139, ¶¶[0087]-[0099]. For instance, a user can use an RDC integrated in the hybrid device to secure the data within the

hybrid device (cell phone) to protect it from loss or theft. Giobbi '139, ¶[0091]. Further the RDC would allow other external PDKs to interact with the hybrid device. Accordingly, a POSITA would have recognized that a mobile device having an integrated RDC and PDK would provide increased security in accessing both assets internal to the mobile device and assets external to the mobile device.

As discussed above in Section IV.B, the '042 Patent, the '289 Patent, and the '960 Patent purport to merely combine existing PDKs and RDCs into a single “hybrid device.” Since each element of the claimed invention (wireless links, PDKs, RDCs, enablement signal) existed long before the priority dates of the '042 Patent, the '289 Patent, and the '960 Patent, a person of ordinary skill in the art would have been motivated to add them as one of a limited number of design options available when implementing a method of enabling access to an application. Moreover, a POSITA would have been motivated to and have a reasonable expectation of success of combining a PDK and RDC into a single Hybrid Device, including doing so was well known both from literature (e.g., Dua) and consumer devices (e.g., cell phones from Nokia, Sony-Ericsson, and HTC). Indeed, combining a PDK and RDC into a single Hybrid Device may entail little more than taking two well known devices or circuit boards found there, potentially connecting them via a single cable, and placing them in the same box without substantially modifying either.

Additional motivation to incorporate any of the concepts claimed in the '042 Patent, the '289 Patent, and the '960 Patent into any primary reference allegedly missing those concepts is set forth below:

a. PDK

As discussed above in Section IV.B,1 (incorporated herein by reference), the '042 Patent, the '289 Patent, and the '960 Patent all describe the use of a “hybrid device,” and the '042 Patent

requires the hybrid device to include an “integrated PDK,” or “personal digital key,” which existed long before the priority dates of the asserted patents. The patents themselves acknowledge multiple examples of personal digital keys, including proximity sensors and location tracking devices that would be used in various secure access applications. *See supra* Section IV.B.1. Moreover, as computing power and memory became cheaper and available in progressively smaller form factors, incorporating storage of user information in smaller devices, such as the claimed hybrid devices, also became more readily available and thus more desirable. For example, including such storage may permit the PDK to serve multiple purposes (e.g., track available bank account balance in addition to providing access to bank account) and facilitate return of lost devices (e.g., by containing the name and address of their owner).

Thus, a POSITA would have been motivated to incorporate a personal digital key into an existing method of enabling access to an application in order to achieve the known and predictable result of storing personal information for transmission. In creating a method of accessing an application, a POSITA would have found it obvious to incorporate existing personal digital keys on the market, such as RFID tags or other proximity sensors with local memories as cited in the patents. A POSITA would have been able to do so with a reasonable expectation of success.

b. RDC

As discussed above in Section IV.B.2 (incorporated herein by reference), the ’042 Patent, the ’289 Patent, and the ’960 Patent all describe the use of a “hybrid device,” and the ’042 Patent and the ’289 Patent require the claimed hybrid device to include an “integrated RDC,” or “receiver-decoder circuit,” which existed long before the priority dates of the asserted patents.

A POSITA would have been motivated to modify an existing method of enabling access to an application with a receiver-decoder circuit to solve the known limitations of “dumb” access

control devices that did not have the ability to process information or run applications themselves. Consistent with the market trend toward integrating smart devices with receiver-decoder circuits into existing authentication schemes, and to achieve the predictable benefit of allowing a device to decrypt encrypted data (thereby allowing for improved transmission security), a POSITA would have had a strong incentive to incorporate any number of known, predictable, commercially available receiver-decoder circuits into a device used for access control. In doing so, a POSITA would have had reasonable expectation of success.

c. Wireless Links

As discussed above in Section IV.B.3 (incorporated herein by reference), the '042 Patent, the '289 Patent, and the '960 Patent all require a “wireless link” to be made with the claimed hybrid device, which existed long before the priority dates of the asserted patents. A POSITA would have been motivated to modify an existing method of enabling access to an application by enabling a device to wirelessly link to another device to solve the known limitations and inconveniences of having to use wired data transfer. A POSITA would have had several readily available means and standard protocols to follow for wireless communications, including Bluetooth, IrDA, and WiFi. Moreover, using wireless communication is more convenient (e.g., no need to retrieve device from briefcase) and removes need for additional ports on, e.g., computers. Thus, equipped with these known, predictable, and commercially available options, a POSITA would have been able to incorporate wireless links into a method for enabling access with a reasonable expectation of success.

d. Access Key

Proxense in its infringement contentions alleges that the Hybrid Device patent claims all require storing user information that can “only be accessed by a corresponding access key provided by an external application.” Infringement Contentions Ex. D at 3-4. Proxense further

alleges that “the RP ID”—which according to Proxense acts as a look up index for retrieving data “is an access key.” *Id.* at 4-5.

If the claims are interpreted to require an “access key” used to decrypt user information stored in memory, then this limitation is obvious. Use of access keys to decrypt data stored in memory was well known in the art, as evidenced at least by the disclosure cited in the accompanying claim charts. Moreover, a POSITA would be motivated to use such access keys for additional security. Especially if a PDK or hybrid device is in a small form factor, it may be lost or stolen, and encrypting data stored thereon using an external key prevents a bad actor from gaining access to user information stored therein. Indeed, this approach is common in computer technology, where entire hard drives may be encrypted and require a user to plug in a separate memory device containing an access key before user information on such an encrypted hard drive may be accessed.

If the claims are interpreted to require an “access key” that is an index for retrieving user information stored in memory, then this limitation is also obvious. Use of access keys as an index to data stored in memory was well known in the art, as evidenced at least by the disclosure cited in the accompanying claim charts. For example, such keys are common in database technology to identify what data is to be retrieved in response to a request. Moreover, use of such keys allows for the requester to exactly specify what data should be included in response or what data should be used as input for further processing, thereby simplifying receiver design and facilitating interoperability between vendors.

VII. INVALIDITY UNDER 35 U.S.C. § 112

Pursuant to the Order Governing Proceedings, Google identifies below grounds of invalidity under 35 U.S.C. § 112.

A. Legal Background Regarding The Indefiniteness, Enablement, And Written Description Requirements

Section 112, ¶ 2 includes a definiteness requirement: “[T]he specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.” 35 U.S.C. § 112, ¶ 2. “[A] patent is invalid for indefiniteness if its claims, read in light of the patent’s specification and prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

The definiteness requirement requires that the claim set forth what the applicant regards as the invention, and do so with sufficient particularity and definiteness. *Allen Eng’g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1348 (Fed. Cir. 2002). Where it would be apparent to one of skill in the art, based on the patent specification, that the “invention” set forth in a claim is not what the patent applicant regarded as the invention, the claim is invalid. *Id.*

35 U.S.C. § 112 further includes an enablement requirement: “The specification shall contain a written description . . . of the manner and process of making and using [the invention] in such full, clear, concise and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same.” 35 U.S.C. § 112, ¶ 1. To satisfy the enablement requirement, the disclosure “must teach those skilled in the art how to make and use the full scope of the claimed invention without ‘undue experimentation.’” *Genentech, Inc. v. Novo Nordisk A/S*, 108 F.3d 1361, 1366 (Fed. Cir. 1997); *MagSil Corp. v. Hitachi Glob. Storage Techs., Inc.*, 687 F.3d 1377, 1381 (Fed. Cir. 2012); *Sitrick v. Dreamworks, LLC*, 516 F.3d 993, 999 (Fed. Cir. 2008). If a specification teaches away from a substantial portion of the claim or does not enable the full scope of the claim, there is no enablement. *AK Steel Corp.*

v. Sollac, 344 F.3d 1234 (Fed. Cir. 2003); *see also MagSil Corp.*, 687 F.3d at 1383-84 (Fed. Cir. 2012).

35 U.S.C. § 112 further includes a written description requirement: “The specification shall contain a written description of the invention” 35 U.S.C. § 112, ¶ 1. “To satisfy the written description requirement, a patent applicant must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention.” *ICU Medical Inc. v. Alaris Medical Systems, Inc.*, 558 F.3d 1368, 1377 (Fed. Cir. 2009) (internal quotation marks and citations omitted); *see also Synthes USA, LLC v. Spinal Kinetics, Inc.*, 734 F.3d 1332, 1340 (Fed. Cir. 2013). “The test [for written description support] requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Based on that inquiry, the specification must describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed.” *Ariad Pharmaceuticals, Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc).

The specification must describe the claimed invention in sufficient detail so that a POSITA can recognize what is claimed. “The appearance of mere indistinct words in a specification or a claim, even an original claim, does not necessarily satisfy that requirement.” *University of Rochester v. G.D. Searle & Co.*, 358 F.3d 916, 923 (Fed. Cir. 2004) (internal quotation marks and citations omitted).

B. Invalidity Grounds Under 35 U.S.C. § 112

Based on Proxense’s Infringement Contentions,, Google identifies grounds upon which it contends that the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. §§ 112 ¶¶ 1, 2 and/or 4. Although its investigation continues, Google believes that the Asserted Claims identified below are invalid for failure to comply with 35 U.S.C. § 112 for at least the following reasons: (1) the specifications of the Patents-in-Suit lack a written description of the

alleged inventions of the Asserted Claims in full, clear, concise, and exact terms as required by 35 U.S.C. § 112 ¶ 1; and/or (2) the specifications of the Patents-in-Suit do not enable the Asserted Claims as required by 35 U.S.C. § 112 ¶ 1; and/or (3) one or more of the Asserted Claims fail to specify a further limitation of the subject matter claimed. Google specifically reserves the right to amend and/or supplement these Invalidity Contentions based on a failure to comply with the requirements of 35 U.S.C. § 112, including, for example, based on supplementation or amendments to Proxense's deficient Infringement Contentions.

The Asserted Claims fail to meet the written description requirement because the alleged inventions claimed therein are not sufficiently described in the specification of the Patents-in-Suit. Specifically, the Asserted Claims fail to meet the written description requirement for at least the terms identified below because, based on those terms, the specifications of the Patents-in-Suit do not adequately convey to those skilled in the art that the inventors had possession of the claimed subject matter as of the filing date. The Asserted Claims additionally fail to meet the enablement requirement because each specification of the Patents-in-Suit does not describe the manner and process of making and using the alleged inventions in the Asserted Claims to enable a person of skill in the art to make and use the full scope of the alleged invention without undue experimentation. Specifically, the Asserted Claims fail to meet the enablement requirement for at least the terms identified below because the specifications of the Patents-in-Suit do not describe the manner and process of making and using the alleged invention in the Asserted Claims. Based on Google's present understanding of the Asserted Claims and Proxense's apparent interpretation of these claims as reflected in its Infringement Contentions, the Asserted Claims may fail to satisfy the requirements of § 112, ¶ 2 because the precise scope of at least the phrases listed below (or

terms contained therein) cannot be determined with reasonable certainty by a POSITA when reading the claims in light of the specification and prosecution history.

The Asserted Claims fail the requirements of 35 U.S.C. § 112 in view of at least the following claim terms and phrases:

Asserted Claim(s)	Claim Term	Invalidity Based on 35 U.S.C. § 112
'730 Patent		
Claim 1	“persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption values”	Lack of Written Description; Lack of Enablement; Indefinite
Claims 1, 15	“integrated device”	Lack of Written Description; Lack of Enablement; Indefinite
Claims 1, 15	“unable to be subsequently altered”	Lack of Written Description; Lack of Enablement
Claim 5	“The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.”	Indefiniteness 35 U.S.C. § 112, ¶ 4
'954 Patent		
Claim 1	“persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value”	Lack of Written Description; Lack of Enablement; Indefinite
Claims 1, 6	“integrated device”	Lack of Written Description; Lack of Enablement
Claims 1, 22	“not capable of being subsequently altered”	Lack of Written Description; Lack of Enablement
'905 Patent		
Claim 1,	“persistently storing biometric data of a legitimate user and an ID code on an integrated device”	Lack of Written Description; Lack of Enablement; Indefinite
Claims 1, 5	“integrated device”	Lack of Written Description; Lack of Enablement

Google reserves the right to modify, amend, or supplement its contentions relating to 35 U.S.C. § 112 as the case progresses including, in particular, in view of any supplemental claim construction order entered by the Court in this matter.

VIII. INVALIDITY UNDER 35 U.S.C. § 101²

To be patentable subject matter under § 101, a claim must be directed to one of four eligible subject matter categories: “new and useful process, machine, manufacture, or composition of matter.” 35 U.S.C. § 101. “Claims that fall within one of the four subject matter categories may nevertheless be ineligible if they encompass laws of nature, physical phenomena, or abstract ideas.” *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980). The Supreme Court established a two-step test for deciding the subject matter eligibility of claims under § 101. *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2355 (2014). First, the claims must be analyzed to determine whether they are drawn to one of the statutory exceptions. *Id.* Claims that invoke generic computer components instead of reciting specific improvements in computer capabilities are abstract under this first step. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016). Second, the elements of the claims must be viewed both individually and as an ordered combination to see if there is an “inventive concept.” *Id.* The mere fact that a claim recites or implies that an abstract idea is implemented using a general-purpose computer does not supply an inventive concept necessary to satisfy § 101. *See Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1355 (Fed. Cir. 2016); *Alice*, 134 S. Ct. at 2357-59.

² The Court’s Order Governing Proceedings only requires Google to “identify the alleged abstract idea, law of nature, and/or natural phenomenon” as well as “each claim element alleged to be well-understood, routine, and/or conventional.” While, in the interest of disclosure, Google has gone beyond what is required by the OGP, its patent ineligibility disclosures are exemplary and nothing herein shall limit or waive Google’s patent ineligibility arguments.

All of the Asserted Claims are directed to ineligible subject matter under 35 U.S.C. § 101 and applicable case law authority.³

A. '730/'954/'905 Patents (Device ID Patents)

Under Proxense's interpretation, the claims of the '730/'954/'905 Patents are directed to a patent-ineligible abstract idea of two-factor authentication, i.e., preventing unauthorized use of a wireless device by verifying both biometric data and the device itself. Specifically, the two abstract concepts defined in the specification as the solution for the problems these patents sought to solve were: (1) verify the user using conventional biometric scanning techniques; and (2) verify the device using a device ID code and third party trusted authority. Combining two abstract ideas does not render either any less abstract. See *RecogniCorp, LLC v. Nintendo Co., Ltd.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017) ("adding one abstract idea ... to another abstract idea ... does not render the claim non-abstract").

³ See, e.g., *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289 (2012); *Trading Techs. Int'l, Inc. v. IBG, LLC*, 921 F.3d 1084 (Fed. Cir. 2019); *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759 (Fed. Cir. 2019); *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161 (Fed. Cir. 2018); *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335 (Fed. Cir. 2018); *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018); *Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329 (Fed. Cir. 2017), *cert. denied*, 139 S. Ct. 378 (2018); *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332 (Fed. Cir. 2017); *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229 (Fed. Cir. 2016); *Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253 (Fed. Cir. 2016); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016); *Genetic Techs. Ltd. v. Merial L.L.C.*, 818 F.3d 1369 (Fed. Cir. 2016); *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363 (Fed. Cir. 2015); *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343 (Fed. Cir. 2015); *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359 (Fed. Cir. 2015); *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343 (Fed. Cir. 2014); *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014); *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350 (Fed. Cir. 2014); *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011).

Indeed, Proxense's counsel admitted in a prior case involving this patent family that "the claimed inventions" are directed to "providing for multiple levels of authentication." See *Proxense, LLC v. Samsung Elecs. Co., Ltd.*, No. 6:21-cv-00210-ADA (W.D. Tex.), ECF No. 35, at 2 (The '730/'954/'905 Patents family is "directed to inventions ensuring biometric data privacy while enabling biometric authentication. The claimed inventions improve on the prior art by providing for multiple levels of authentication, such that a user is verified as properly in possession of a biometric access instrumentality, and also biometrically verified as authorized to access sensitive and/or secure resources.").

The '730/'954/'905 Patents describe biometric authentication of a user of a wireless device using a generic "computerized authentication" system that provides rudimentary access to resources such as an ATM and other locked areas, including software login. The '730/'954/'905 Patents purport to solve the problem of users having to "memorize or otherwise keep track of the[ir] credentials," while providing security from illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." But this type of biometric authentication system was known years before the '730/'954/'905 Patents were filed. Indeed, the '730/'954/'905 Patents merely recite the well-known concept of verifying biometric data and authenticating a user's device using a third party trusted authority. Thus, consistent with Proxense's description of its alleged inventions, the claims are directed to the abstract idea of verifying a user's identity using biometrics and authenticating the user's device using a third party trusted authority.

There are no elements of the claims that transform the claims into a patent-eligible application of this abstract idea or provide the necessary inventive concept. All limitations of the claims merely involve well-understood, routine, conventional activity and implementations

previously used by those in the field at the time of the alleged invention as demonstrated at least by the prior art in the exhibits attached. Indeed, when describing implementation of the claimed abstract idea, the '730/'954/'905 Patents merely recite a generic arrangement of known, conventional components. As Proxense's counsel has admitted in prior cases involving other members of the '730/'954/'905 Patents' family, the Asserted Patents are not limited to a particular means of authenticating a user. See *Proxense, LLC v. Samsung Elecs. Co., Ltd.*, No. 6:21-cv-00210-ADA (W.D. Tex.), ECF No. 35, at 1 ("The inventions ... allow users to carry, control, and protect their own personal data on devices like mobile phones, which allows for secure financial transactions using those devices. Biometric authentication and use of remote (e.g., web-based) applications requires an element of trust between the user and the service provider"); *id.* ("The inventions of the patents-in-suit address such issues by providing ways to use biometric information securely to access and/or utilize private, sensitive information."). Moreover, the only alleged difference between the prior art and the claims of these and related patents identified by Proxense across multiple proceeding, including the *Samsung* litigation and IPR2021-01438; IPR2021-01439; IPR2021-01444; IPR2021-01447; IPR2021-01448; IPR2024-00232; IPR2024-00233; IPR2024-00234; Reexamination Nos. 90/015,052, 90/015,053, 90/015,054, was the use of a third party trusted authority. But such use is an abstract idea and thus cannot supply an inventive concept under step two of the *Alice* framework. *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018) ("[A] claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention "significantly more" than that ineligible concept.").

B. '042/'289/'960 Patents (Hybrid Device Patents)

Under Proxense's interpretation, the claims of the '042/'289/'960 Patents are directed to a patent-ineligible concept of exchanging information between two devices as part of enabling

access to an application, function, or service. The Federal Circuit has confirmed that such claims are invalid. *See, e.g., ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 768 (Fed. Cir. 2019) (“the invention of the patent is nothing more than the abstract idea of communication over a network for interacting with a device”); *Chamberlain Group, Inc. v. Techtronic Industries Co.*, 935 F.3d 1341, 1348 (Fed. Cir. 2019) (“[W]e find that the asserted claims are drawn to the abstract idea of wirelessly communicating status information about a system”).

For example, in *Universal Secure Registry LLC v. Apple, Inc.*, 10 F.4th 1342 (Fed. Cir. 2021), the Federal Circuit held that the patent claims were directed to the abstract idea of combining multiple conventional authentication techniques for verifying the identity of a user to facilitate a financial transaction. The patent specifications disclosed that biometric authentication, multi-factor authentication, and using multiple devices to authenticate were all conventional authentication techniques. The claims, then, were simply directed to combining these long-standing, well-known authentication techniques to achieve the expected result of increased security no greater than the sum of the security provided by each technique alone. Under *Alice* step two, the Federal Circuit held that these claims did not recite an inventive concept because the combination of long-standing conventional methods of authentication yielded expected results of an additive increase in security, and nothing in the record suggested an additional technological improvement.

The claims of the '042/'289/'960 patent are no different than the claims in *Universal Secure Registry LLC*. The '042/'289/'960 use their own nomenclature such as PDK and RDC (terms which are found in the prior art such as Giobbi '139 and Giobbi '157) to identify different components of the claimed invention but these components merely represent a wireless decoder device and a device capable of storing secured information. These are basic, well-known

technologies and the claims do not combine them in any special way producing unknown or unexpected results. All limitations of the claims merely involve well-understood, routine, conventional activity and implementations previously used by those in the field at the time of the alleged invention.

Indeed, in cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself. For example, in *Secured Mail Solutions LLC v. Universal Wilde, Inc.*, the Federal Circuit held that claims directed to using a marking (e.g., a conventional barcode) affixed to the outside of a mail object to communicate information about the mail object, including claims reciting a method for verifying the authenticity of the mail object, were abstract. 873 F.3d 905, 907, 910–11 (Fed. Cir. 2017). The Court explained that the claims were not directed to specific details of the barcode or of the equipment for generating and processing the barcode. Nor was there a description of how the barcode was generated, or how that barcode was different from long-standing identification practices. At step two, the Federal Circuit determined that there was no inventive concept that transformed the claimed abstract idea into a patent-eligible application of the abstract idea. *See id.* at 912. Again, the Court explained that the claims recited well-known and conventional ways to verify an object using a barcode and to allow generic communication between a sender and recipient using generic computer technology, and that the patents themselves suggested that all the hardware used was conventional. *See id.*

In *Electronic Communication Technologies, LLC v. ShoppersChoice.com, LLC*, the Federal Circuit drew a similar conclusion about claims focused on monitoring the location of a “mobile thing” and using authentication software to increase security. 958 F.3d 1178, 1181 (Fed. Cir. 2020). As to the authentication limitations—“namely, enabling a first party to input

authentication information, storing the authentication information, and providing the authentication information along with the advance notice of arrival to help ensure the customer that the notice was initiated by an authorized source”—the Federal Circuit determined that these limitations were themselves abstract and thus were not an inventive concept. *Id.* The Court pointed to the specification, which stated that the claimed “authentication information” could be essentially any information recognizable to the party being contacted. *Id.* Businesses have long been recording customer information that would qualify as authentication information as broadly defined in the specification. *See id.* at 1182.

Similarly, in *Solutran, Inc. v. Elavon, Inc.*, the Federal Circuit held ineligible claims that recited a method for electronically processing checks, which included electronically verifying the accuracy of a transaction to avoid check fraud, because the claims were directed to a long-standing commercial practice of crediting a merchant’s account as soon as possible. 931 F.3d 1161, 1163, 1167 (Fed. Cir. 2019). The Court recognized that the claims only recited conventional steps that were not directed to an improvement to the way computers operate, noting that the patent specification explained that “verifying the accuracy of the transaction information ... was already common.” *Id.* at 1167. Beyond that, at step two, the Federal Circuit rejected the argument that reordering these conventional steps constituted an inventive concept, and held that using a general-purpose computer and scanner to perform the conventional activities of transaction verification does not amount to an inventive concept. *Id.* at 1168–69.

Finally, in *Prism Technologies LLC v. T-Mobile USA, Inc.*, the claims broadly recited “receiving” identity data of a client computer, “authenticating” the identity of the data, “authorizing” the client computer, and “permitting access” to the client computer. 696 F. App’x 1014, 1016 (Fed. Cir. 2017). The Federal Circuit held that the claims at issue were directed to the

abstract idea of “providing restricted access to resources” because the claims did not cover a “concrete, specific solution.” *Id.* at 1017. Rather, the claims merely recited generic steps typical of any conventional process for restricting access, including processes that predated computers. *Id.* At step two, the Federal Circuit determined that the asserted claims recited conventional generic computer components employed in a customary manner such that they were insufficient to transform the abstract idea into a patent-eligible invention. *Id.* Like *Prism Technologies*, here, there are no elements of the claims that transform the claims into a patent-eligible application of this abstract idea or provide necessary inventive concept.

The '960 patent is especially invalid under *Alice* because it does not even claim the basic hardware found in the '042 and '289 patent claims (PDK, RDC, and hybrid device). These claims are directed to the even more basic concept of allowing access in response to a signal received from another device.

IX. OBVIOUSNESS-TYPE DOUBLE PATENTING

Google contends that the '730 patent is invalid for obviousness-type double-patenting (ODP) over the claims of the '905 and '954 patents. The '905 and '954 patents are set to expire on December 20, 2025, but the '730 patent received a patent term adjustment and is set to expire on July 15, 2028. As the Federal Circuit has recently held, “ODP for a patent that has received PTA, regardless whether or not a terminal disclaimer is required or has been filed, must be based on the expiration date of the patent after PTA has been added.” *In re: Collect, LLC*, No. 2022-1293, 2023 WL 5519716, at *9 (Fed. Cir. Aug. 28, 2023). Moreover, the claims of all three patents are directed to at most obvious variations of the claims in each other. Thus, the '730 patent has received an “inappropriate timewise extension” past the date of December 20, 2025. *Id.* at *10.

X. IMPROPER PRIORITY CLAIM FOR ADDITION OF NEW MATTER

Google contends that Proxense has improperly identified the '905 and '954 patents as “continuations” of the '730 patent, because they introduce concepts not previously present in the '730 specification. As such, the '905 and '954 patents cannot be entitled to the priority date of the '730 patent. *See Litton Sys., Inc. v. Whirlpool Corp.*, 728 F.2d 1423, 1437–38 (Fed. Cir. 1984).

In order to gain the benefit of the filing date of an earlier application, “each application in the chain leading back to the earlier application must comply with the written description requirement of 35 U.S.C. § 112.” *Zenon Environmental, Inc. v. U.S. Filter Corp.*, 506 F.3d 1370, 1378, 85 U.S.P.Q.2d 1118, 1123–24 (Fed. Cir. 2007). Thus, in order for the '905 and '954 patents to be entitled to the priority date of the '730 patent, there must be “sufficient information in the original disclosure to show that the inventor possessed the invention at the time of the original filing.” *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1320 (Fed. Cir. 2003). Having been filed as continuation applications, the '905 and '954 must be “based solely on the disclosure of a parent application” and cannot add new matter. *Applied Materials, Inc. v. Advanced Semiconductor Materials America, Inc.*, 98 F.3d 1563, 40 U.S.P.Q.2d 1481 (Fed. Cir. 1996) (Mayer, J., *concurring*).

However, Proxense added several new disclosures to the '954 and '905 patents. For example, when Proxense filed the application that matured into the '954 patent, it added an express definition for the term “integrated device” and a list of exemplary devices that qualify as an “integrated device”—none of which appears in the '730 patent:

In one embodiment, the biometric key 100 is integrated into another object or device. A device having an integrated biometric key 100 is occasionally referred to herein as an “integrated device.” For example, in one embodiment, the biometric key 100 is integrated into a mobile phone (e.g. a cellular phone or

smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key 100 unobtrusive to carry.

'954 patent at 4:6-14.

By adding a definition of “integrated device,” thereby changing the scope of this claim term, the '954 and '905 patent added and claimed new subject matter absent from the '730 patent. In addition, the '954 and '905 patents disclosed and claimed that the “integrated device” “comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob” ('954 patent at 4:10-14; '954 patent claims 6, 25; '905 patent claims 5, 12, 15), whereas the '730 patent only disclosed that “biometric key 100 comprises a modified key fob” ('730 patent at 3:53-54). That the '954 and '905 patents disclosed and claimed embodiments (“a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch”) not found in the '730 patent confirms that they added new matter. *See TurboCare Div. of Demag Delaval Turbomachinery Corp. v. Gen. Elec. Co.*, 264 F.3d 1111, 1119 (Fed. Cir. 2001) (finding claims improperly added new matter where the original disclosure was “completely lacking in any description” of the embodiment described in the claims).

The '954 and '905 patent also added new matter in the form of disclosure and claims specifying that the application to which access is controlled can be “a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.)” or “medical information such as a medical record, insurance information or other healthcare information.” '954 patent at 6:22-26; '905 patent at 6:24-28.

By adding a written description of the above to the '954 patent application and its progeny, Proxense introduced new matter that is not part of the '730 patent. *See, e.g., Dart Indus., Inc. v. Banner*, 636 F.2d 684, 688 (D.C. Cir. 1980) (“An addition to a patent specification constitutes ‘new matter’ when it changes the invention disclosed or introduces a concept not

previously present in that specification.”) (citing *In re Anderson*, 471 F.2d 1237, 1244 (C.C.P.A.1973); *In re Oda*, 443 F.2d 1200, 1203-05 & n.2 (C.C.P.A.1971)). Thus, the ’954 and ’905 patents are not proper “continuations” of the ’730 patent and cannot be entitled to its priority date. Rather, the earliest priority date that the ’954 and ’905 patents are possibly entitled to is the filing date of the application for the ’954 patent, which added this new matter, on December 10, 2012.

XI. DOCUMENT PRODUCTION ACCOMPANYING INVALIDITY CONTENTIONS

Google previously produced the documents required under the parties’ Scheduling Order (Dkt. 31 at 1). In addition, Google is producing all prior art referenced in these contentions, as well as additional technical documents showing the operation of the prior art products. Google is also making available for inspection physical examples of the prior art and any prior art source code.

Dated: March 18, 2024

/s/ John McKee

Kevin Hardy
kevinhardy@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street, NW, Suite 900
Washington, D.C. 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Iman Lordgooei
imanlordgooei@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

John McKee
johnmckee@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Telephone: (212) 849-7000
Facsimile: (212) 849-7100

Counsel for Defendant

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on March 18, 2024, all counsel of record who have appeared in this case are being served with a copy of the foregoing via email.

Dated: March 18, 2024

/s/ John McKee
John McKee