UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/015,053	06/08/2022	9298905	2090-0002-REX	7424

142179 7590 12/21/2022

Hard IP LLC (General)
10 Notch Hill Drive
Livingston, NJ 07039

EXAMINER	
RIMELL, SAMUEL G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
12/21/2022	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

December 21, 2022

MARISSA R. DUCCA
QUINN EMANUEL URQUHART & SULLIVAN. LLP
1300 I STREET, NW SUITE 900
WASHINGTON, DC 20005

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 90015053
PATENT NO. : 9298905
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Hard IP LLC (General)
10 Notch Hill Drive
Livingston, NJ 07039

(For Patent Owner)

Marissa R. Ducca
Quinn Emanuel Urquhart and Sullivan, LLP
1300 I Street, NW
Suite 900
Washington, DC 20005

(For Third Party Requester)

In re Giobbi
U.S. Patent No.: 9,298,905 B1
Ex Parte Reexamination Proceeding
Control No.: 90/015,053
Filed: June 8, 2022

: **DECISION**
: **ON**
: **PAPER**

This decision addresses third party requester's August 5, 2022 paper entitled "Response to Petition Under 1.183 to Suspend and/or Waive Rules 37 C.F.R. § 1.530(a) and (c)" (opposition). Third party requester's opposition is before the Office of Patent Legal Administration (OPLA) for consideration.

On July 22, 2022, patent owner filed a petition entitled "Petition Under 1.183 to Suspend and/or Waive Rules 37 C.F.R. § 1.530(a) and (c)" (petition). The petition sought waiver of 37 CFR 1.530(a) and (c) to permit the Office to consider a future patent owner petition requesting the Office to reject the request in the present reexamination proceeding pursuant to 35 U.S.C. 325(d). On August 1, 2022, OPLA issued a decision: (i) granting patent owner's petition under 37 CFR 1.183 to waive 37 CFR 1.530(a) and (c) for entry and consideration of any information regarding § 325(d) issues set forth in the petition itself when determining whether to order reexamination to the extent sufficient time remained, and (ii) finding premature patent owner's request for waiver of the rules to permit the Office to enter and consider a future petition directed to issues under § 325(d). On August 2, 2022, the Central Reexamination Unit (CRU) issued an "Order Granting Request for *Ex Parte* Reexamination," in which the examiner included a discussion in support of the examiner's determination that "a discretionary denial of reexamination pursuant to 35 USC 325(d) is not implicated...."[1] On August 5, 2022, requester filed the opposition, requesting that the CRU "reject Patent Owner's petition and proceed with *ex parte* reexamination."[2]

In general, requester is permitted to file a paper in opposition to a patent owner petition to reject a request and deny reexamination pursuant to 35 U.S.C. 325(d), just as the requester is permitted to file a paper in opposition to a patent owner petition to vacate a reexamination order under 35 U.S.C. 304 (and deny reexamination) on the basis that the order is an *ultra vires* action on the part of the Office.[3] However, here, the requester responded to the patent owner's petition after it was already decided and

[1] *See* "Order Granting Request for *Ex Parte* Reexamination," August 2, 2022, page 12 (the order).
[2] Opposition, page 9.
[3] *See, e.g.*, MPEP § 2246, subsection II.

after the order granting *ex parte* reexamination was issued.[4] Further, the relief sought by the opposition has already been granted (i.e., the Office did not exercise discretion under § 325(d), and proceeded with reexamination). Accordingly, requester's August 5, 2022 opposition is **moot** but will remain in the record.

Any questions concerning this communication should be directed to Andrea Grossman, Patent Examination Policy Advisor, Office of Patent Legal Administration, at (571) 270-3314, or the undersigned, at 571-272-7717.

/Nicole D. Haines/

Nicole D. Haines
Senior Legal Advisor
Office of Patent Legal Administration December 21, 2022

[4] It is noted that patent owner filed an additional petition addressing 35 U.S.C. 325(d) on September 20, 2022, and requester filed an opposition to the September 20, 2022 petition on October 4, 2022. These papers will be addressed in due course.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**Corrected Certificate of Service**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The undersigned herby certifies that, as set forth below, a copy of the Third Party Requestors Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 was served via First Class mail and, pursuant to the parties' stipulation, via electronic service.

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on December 8, 2022, a copy of the Third Party Requestors Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 was served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
125 Park Avenue, 25th Floor
New York, NY 10017

The undersigned hereby certifies that a confirmation copy of the Third Party Requestors Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 were sent via Fedex on December 9, 2022 and via First Class Mail on December 19, 2022 to the addresses listed below:

Kinza Hecht
Woo-Hyeong Chung
Hard IP LLC
10 Notch Hill Drive
Livingston, NJ 07039
UNITED STATES

Dated: December 19, 2022

By: */s/ James M. Glass*
James M. Glass
Reg. No. 46,729

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/015,053	**12/19/2022 03:02:59 PM ET**	**2090-0002-REX**

Title of Invention

Biometric personal data key (PDK) authentication

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	9298905
CONFIRMATION #	7424	FILED BY	James Glass
PATENT CENTER #	61320820	FILING DATE	06/08/2022
CUSTOMER #	142179	FIRST NAMED INVENTOR	- 9298905
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
905 Opp COS.pdf	2	Reexam Certificate of Service	115 KB
905 Reply COS.pdf	2	Reexam Certificate of Service	119 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
905 Opp COS.pdf	1B932AD1F83E57EE640B72D00EB4656BF4B65FC4C3842B709 EF24FD01D4BB500A4B21B79429BC53B150C326D523F4F3ED9 2EC462D373C21E8BA0598DD2AA79FD
905 Reply COS.pdf	033992A8A4CC343434FC3CB7061BAE1CFB09A7B8B23381FB6

7761478AF22575729D492A7C62412D0969205BFCCC175BE8C
C2753AF4634217D2F8C6D675D764B7

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**Corrected Certificate of Service**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The undersigned herby certifies that, as set forth below, a copy of Opposition to Patent Owner's Second Petition was served via First Class mail and, pursuant to the parties' stipulation, via electronic service.

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on October 4, 2022, a copy of Opposition to Patent Owner's Second Petition was served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
125 Park Avenue, 25th Floor
New York, NY 10017

Further, the undersigned hereby certifies that a confirmation copy of the Opposition to Patent Owner's Second Petition were sent via Fedex on December 9, 2022 and via First Class Mail on December 19, 2022 to the addresses listed below:

Kinza Hecht
Woo-Hyeong Chung
Hard IP LLC
10 Notch Hill Drive
Livingston, NJ 07039
UNITED STATES

Dated: December 19, 2022

By: */s/ James M. Glass*
James M. Glass
Reg. No. 46,729

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**Corrected Certificate of Service**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on December 8, 2022, a copy of the Third Party Requester's Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 were served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
10 Notch Hill Drive
Livingston, NJ 07039

The undersigned hereby certifies that on December 9, 2022, a confirmation copy of the Third Party Requester's Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 were sent via Fedex to the addresses listed below:

Kinza Hecht
Woo-Hyeong Chung
Hard IP LLC
10 Notch Hill Drive
Livingston, NJ 07039
UNITED STATES

Dated: December 9, 2022

By: */s/ James M. Glass*
James M. Glass
Reg. No. 46,729

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**Corrected Certificate of Service**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on October 4, 2022, a copy of Opposition to Patent Owner's Second Petition was served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
10 Notch Hill Drive
Livingston, NJ 07039

Further, the undersigned hereby certifies that on December 9, 2022, a confirmation copy of the Opposition to Patent Owner's Second Petition was sent via Fedex Priority Overnight to the address listed below:

Kinza Hecht
Woo-Hyeong Chung
Hard IP LLC
10 Notch Hill Drive
Livingston, NJ 07039
UNITED STATES

Dated: December 9, 2022

By: */s/ James M. Glass*
James M. Glass
Reg. No. 46,729

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/015,053	**12/09/2022 05:26:57 PM ET**	**2090-0002-REX**

Title of Invention

Biometric personal data key (PDK) authentication

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	9298905
CONFIRMATION #	7424	FILED BY	James Glass
PATENT CENTER #	61281115	FILING DATE	06/08/2022
CUSTOMER #	142179	FIRST NAMED INVENTOR	- 9298905
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
905 Requester Reply Corrected COS.pdf	2	Reexam Certificate of Service	142 KB
905 Opp to 2nd Petition Corrected COS.pdf	2	Reexam Certificate of Service	145 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
905 Requester Reply Corrected COS.pdf	328589E8E8EC6605B2552D590FD333E7280EF3587CE942693F 1A38FE6FEB77919E0ADCF386F47D318B86419272752E78D43F 9723F91EA59D4CCFC1CA23A3CDF4

905 Opp to 2nd Petition Corrected COS.pdf	EECC3134C006A4764309034B3FF0AF23F8AD8B96797455BD730531801070E285514E7D6E05FC19ED787960D06B31E23CF6FCD70B5196E269CB4467979FEFFE0B

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Network Working Group
Request for Comments: 3601
Category: Standards Track

C. Allocchio
GARR-Italy

September 2003

Text String Notation for Dial Sequences and Global Switched Telephone Network (GSTN) / E.164 Addresses

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This memo describes the full set of notations needed to represent a text string in a Dial Sequence. A Dial Sequence is normally composed of Dual Tone Multi Frequency (DTMF) elements, plus separators and additional "actions" (such as "wait for dialtone", "pause for N secs", etc.) which could be needed to successfully establish the connection with the target service: this includes the cases where subaddresses or DTMF menu navigation apply.

1. Introduction

Since the very first devices interacting with GSTN services appeared, a need for a unique text string representation of commonly called telephone numbers, and more generally DTMF sequences and actions, was foreseen.

This memo describes the full text string representation method. This specification was explicitly created to provide an easy, unique and complete reference which MUST be used by all other specifications needing a text string representation for a Dial Sequence.

The specification was collected directly from Dial Sequence definitions which are already described in existing Standard Track specifications (such as [6] [7] [8] [9]), and is fully synchronized with them. Full compatibility is thus assured, and as a consequence, this specification results in a compendium of existing definitions.

This notation is a fully compatible compendium of existing notations, and should be used in all specifications needing a text string representation of a Dial Sequence.

Although the commonly called "telephone numbers" are normally used to generate a Dial Sequence when establishing a connection, the full abstract E.164 addresses [2], i.e., the universal addressing on the Global Switched Telephone Network (GSTN), have further elements which cannot be dialled. Thus abstract E.164 addresses cannot be fully converted into a Dial Sequence or fully represented using this notation.

1.1. Terminology and Syntax conventions

In this document the formal definitions are described using ABNF syntax, as defined in [3]. This memo also uses some of the "CORE DEFINITIONS" defined in "APPENDIX A - CORE" of that document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [4].

The following terms are also defined in this document:

Dial Sequence:
a series of DTMF elements and human or device "actions";

phone-string:
a text representation of a Dial Sequence;

GSTN address: a commonly called "telephone number" on the GSTN, i.e., a diallable subset of an E.164 abstract address or any private numbering schema diallable address;

gstn-phone:
a text representation of a GSTN address;

subaddr-string:
a text representation of a GSTN subaddress (which includes ISDN subaddresses [2] and T.33 subaddresses [5]);

post-dial:
a text representation of a post dialling sequence.

2. The "Dial Sequence" definition

The possible elements composing a Dial Sequence can vary from a minimum number, up to a really large and complex collection: in fact, the sequences already needed to dial a gstn-phone, which is a subset of the generic Dial Sequence, well represents this variety and complexity of cases.

In particular, a Dial Sequence is composed by:

- "DTMF elements": normally available as "keys" on numeric keypads of dialling devices;
- "actions": normally performed by the agent (human or device) composing the Dial Sequence;
- "separators": used only to improve human readability of a Dial Sequence.

2.1. The "phone-string" definition

The text representation of the Dial Sequence elements is defined in the phone-string specification:

```
phone-string = 1*( DTMF / pause / tonewait / written-sep )

DTMF = ( DIGIT / "#" / "*" / "A" / "B" / "C" / "D" )
                ; special DTMF codes like "*", "#", "A", "B",
                ; "C", "D" are defined in [1].
                ; Important Note: these elements only apply for
                ; alphabetic strings used in DTMF operations.
                ; They are NOT applicable for the alphabetic
                ; characters that are mapped to digits on phone
                ; keypads in some countries.

pause = "p"

tonewait = "w"

written-sep = ( "-" / "." )
```

Note:
DTMF are the "DTMF elements", pause and tonewait are the "actions" and written-sep are the "separators".

The "pause" and "tonewait" elements interpretation of the phone-string depends on the specific devices and implementation using the specification. Thus their exact meaning is not mandated in this

document. The next section provides some examples drawn from common practice. Both "pause" and "tonewait" are case insensitive.

Implementation of "pause" and "tonewait":

- one instance of a "pause" SHOULD be interpreted as a pause of one second between the preceding and succeeding dial string elements;

- a "tonewait" SHOULD be interpreted as a pause that will last until the calling party hears a dial tone or another indication that more dial string characters may be processed. An off-hook indication MAY also be interpreted as this kind of indication (meaning that the audio channel has been opened to the receiving party);

- because these characters are not a part of the GSTN subscriber address (telephone number) per se, any dial string characters that succeed either a "pause" or "tonewait" SHOULD be sent using DTMF signalling.

The use of written-sep elements is allowed in order to improve human readability of the phone-string. The written-sep are elements which can be placed between dial elements, such as digits etc. Any occurrences of written-sep elements in a phone-string MUST NOT result in any action. Conformant implementations MAY drop or insert written-sep into the phone-string they handle.

The phone-string definition is used in the following sections to explicitly describe the encoding of some specific subcases where it applies.

3. The "gstn-phone" definition

In order to access a GSTN address, a human or a device must perform a Dial Sequence. Thus, a GSTN address can be represented using the phone-string elements. In particular, diallable E.164 numeric addresses [2] represent a limited subset of all possible GSTN addresses, while the complete complex case needs a full encoding schema, as it also includes a local or private addressing schema.

In order to describe this distinction and provide anyhow a complete encoding schema, the following definition of "gstn-phone" is provided:

```
gstn-phone = ( global-phone / local-phone )
```

3.1. The "global-phone" definition

The purpose of the global-phone element is to represent diallable E.164 numeric addresses. As such, it uses a subset of a phone-string definition only.

The syntax for a global-phone element is as follows:

```
global-phone = "+" 1*( DIGIT / written-sep )
```

Any other dialling schemes MUST NOT use the leading "+" defined here. The "+" sign is strictly reserved for the standard "global-phone" syntax, and, even if not specifically part of the phone-string definition, it is needed to uniquely label a global-phone.

3.2. The "local-phone" definition

The local-phone element is intended to represent the set of possible cases where the global-phone numbering schema does not apply. Given the different and complex conventions currently being used in the GSTN system, the local-phone definition supports a large number of elements.

The detailed syntax for local-phone elements is as follows:

```
local-phone =  [ exit-code ] dial-number

local-phone =/ exit-code [ dial-number ]

exit-code = phone-string
            ; this will include elements such as the digit to
            ; access outside line, the long distance carrier
            ; access code, the access password to the service,
            ; etc...

dial-number = phone-string
            ; this is in many cases composed of different elements
            ; such as the local phone number, the area code
            ; (if needed), the international country code
            ; (if needed), etc...
```

Notes:

The "+" character is reserved for use in a global-phone and MUST NOT be used in a local-phone string;

Please note that a local-phone string MUST NOT be a null string, i.e., at least an exit-code, or a dial-number or both MUST be present.

4. The "subaddr-string" definition

In GSTN service, there are cases where a subaddress is required to specify the final destination. To specify these subaddresses, a Dial Sequence is also used, and thus the "subaddr-string" can be encoded as:

```
subaddr-string = phone-string
```

Note:
Within actual uses of subaddresses, some specific services can limit the possible set of phone-string elements allowed. In particular, there are ISDN subaddresses [2] [8], which restrict the phone-string elements to 1*(DIGIT / written-sep) and service specific subaddresses, like the fax service T.33 subaddress [5] [7], which restrict phone-string elements to 1*(DIGIT).

5. The "post-dial" definition

In some cases, after the connection with the destination GSTN device has been established, a further dialling sequence is required to access further services. A typical example is an automated menu-driven service using DTMF sequences. These cases may be represented using the "post-dial" definition below:

```
post-dial = phone-string
```

6. Examples

In order to clarify the specification we present, here are a limited set of examples. Please note that all the examples are for illustration purposes only.

A GSTN address in Italy, dialled from U.S.A., using local-phone, without written-sep:

```
01139040226338
```

A GSTN address in Germany, using global-phone and written-sep ".":

```
+49.81.7856345
```

A GSTN address in U.S.A. using global-phone and written-sep "-":

```
+1-202-455-7622
```

A post-dial sequence, pausing, dialling 1, waiting for dial tone, dialling 7005393, waiting again for dial tone and dialling 373; note the use of four "p" elements (pppp) to specify a longer initial pause:

```
ppppw1w7005393w373
```

A Dial Sequence in Italy (long distance call), using local-phone, with exit-code "9", long distance access "0", area code "40", pause "p" and written-sep ".":

```
9p040p22.63.38
```

A Dial Sequence using exit-code "0", a wait for dial tone, local-phone for an International "800" toll-free number dialled from Belgium (international prefix "00"), and a post-dial sequence to access a voice mailbox with userID "334422" and Personal Identification Number (PIN) code "1234":

```
0w00800-39380023pp334422p1234
```

7. Conclusions

This proposal creates a full standard text encoding for Dial Sequences, including GSTN and diallable E.164 addresses, and thus provides a unique common representation method both for standard protocols and applications.

Some definitions, like these corresponding to an alias of the generic phone-string element, are somewhat a theoretical distinction; however they are useful to provide a more subtle distinction, allowing other specifications to be more exact in a consistent way.

The proposal is consistent with existing standard specifications.

8. Security Considerations

This document specifies a means to represent Dial Sequences, which could include GSTN addresses and private codes sequences, like Personal Identification Numbers, to access special services. As these text strings could be transmitted without encoding inside protocols or applications services, this could allow unauthorized people to gain access to these codes. Users SHOULD be provided methods to prevent this disclosure, like code encryption, or masquerading techniques: out-of-band communication of authorization information or use of encrypted data in special fields are the available non-standard techniques.

9. Collected ABNF Syntax

In this section we provide a summary of ABNF specifications.

```
phone-string = 1*( DTMF / pause / tonewait / written-sep )

DTMF = ( DIGIT / "#" / "*" / "A" / "B" / "C" / "D" )

written-sep = ( "-" / "." )

pause = "p"

tonewait = "w"

gstn-phone = ( global-phone / local-phone )

global-phone = "+" 1*( DIGIT / written-sep )

local-phone =  [ exit-code ] dial-number

local-phone =/ exit-code [ dial-number ]

exit-code = phone-string

dial-number = phone-string

subaddr-string = phone-string

post-dial = phone-string
```

10. References

10.1. Normative References

[1] ETSI I-ETS 300,380 - Universal Personal Telecommunication (UPT): Access Devices Dual Tone Multi Frequency (DTMF) sender for acoustical coupling to the microphone of a handset telephone (March 1995).

[2] ITU E.164 - The International Public Telecommunication Numbering Plan E.164/I.331 (May 1997).

[3] Crocker, D. Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] ITU T.33 - Facsimile routing utilizing the subaddress; recommendation T.33 (July, 1996).

10.2. Informative References

[6] Allocchio, C., "Minimal GSTN address format in Internet Mail", RFC 3191, October 2001.

[7] Allocchio, C., "Minimal FAX address format in Internet Mail", RFC 3192, October 2001.

[8] Allocchio, C., "GSTN Address Element Extensions in E-mail Services", RFC 2846, June 2000.

[9] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806, April 2000.

11. Author's Address

Claudio Allocchio
GARR
c/o Sincrotrone Trieste
SS 14 Km 163.5 Basovizza
I 34012 Trieste
Italy

Phone: +39 040 3758523
Fax: +39 040 3758565
X.400: C=it;A=garr;P=garr;S=Allocchio;G=Claudio;
EMail: Claudio.Allocchio@garr.it

12. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/015,053	**12/08/2022 09:12:22 PM ET**	**2090-0002-REX**

Title of Invention

Biometric personal data key (PDK) authentication

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	9298905
CONFIRMATION #	7424	FILED BY	James Glass
PATENT CENTER #	61276366	FILING DATE	06/08/2022
CUSTOMER #	142179	FIRST NAMED INVENTOR	- 9298905
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 4

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
905 Requester Reply.pdf	11	Reexam Timely Requester's Reply to an Owner's Statement	245 KB
905 Requester Reply COS.pdf	1	Reexam Certificate of Service	114 KB
Ex1016rfc3601.pdf	10	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	25 KB
Ex1017ModemSounds.pdf	7	Reexam - Affidavit/Declaration/Exhibit Filed by 3rd Party	774 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
905 Requester Reply.pdf	0EDE6E83215B8C4D613B7C17A2C6FE76AADD86210A95DAFA98E9B7429175D9DEC2B61C4CE2D5E8EFC4EA750F8D271C1CBCB6E7940720486BAD98ACC7F8DDE51E
905 Requester Reply COS.pdf	3F729EFAAF71D24205D28950AFC6F407EAB885FD20D867EAAE30B7B1F02C5B76279DA5A8A6EBA7EE14D8C4BB4088E4B0C05EA62180065186B249B6ACE8F83818
Ex1016rfc3601.pdf	953C8C9533B6B8217AD7704A6C4728DF9E5545B271753344ED2DDF15DEE48D80EEAD95201D4647C36FDA5109BDA0029738BCC6A364274E8958D3F9A8C2B01BAE
Ex1017ModemSounds.pdf	2B475396D035CC95CBD34492A7ACC3CCDA90ED2FEC2610333754CC074AC88FA54AA8A40E0D31ACB6FDA20B0412AD5A1EF83EBA77BB09F58EABEBCF4F8FE1022C

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**REPLY TO PATENT OWNER'S RESPONSE UNDER 35 U.S.C. §304**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Samsung Electronics America, Inc. ("Samsung" or "Requestor") hereby responds to Patent Owner's Response under 35 U.S.C. §304 requesting termination of the above-captioned *ex parte* reexamination of claims 1-18 (the "Challenged Claims") of U.S. Patent No. 9,298,905 ("the '905 patent"). For the reasons described herein, the above-captioned *ex parte* reexamination should continue and find the Challenged claims invalid.

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	LUDTKE DISCLOSES A "THIRD PARTY TRUSTED AUTHORITY" UNDER THE PTAB'S CONSTRUCTION	1
III.	LUDTKE DISCLOSES AN "ACCESS MESSAGE"	5
IV.	CONCLUSION	8

I. INTRODUCTION

The CRU's finding that Ludtke discloses both a "third party trusted authority" and an "access message" was correct. This is true under both the Board's *Phillips* construction of "third-party trusted authority" and under the BRI construction for the term. PO's arguments in the Statement misconstrue the CRU's findings and the teachings of the prior art. But, as discussed below, the CRU's sound reasoning, grounded in the express teachings of the prior art identified in its Order, confirms that the challenged claims are unpatentable over the submitted prior art. Moreover, even if PO's arguments are correct (they are not), PO fails to address the additional examples of a "third-party trusted authority" and "access message" provided in Samsung's Request, leaving Samsung's arguments unrebutted. Accordingly, Patent Owner's Statement should be rejected and reexamination should continue.

II. LUDTKE DISCLOSES A "THIRD PARTY TRUSTED AUTHORITY" UNDER THE PTAB'S CONSTRUCTION

The PTAB construed "***third-party trusted authority***" as requiring "***an entity separate from the parties to a transaction***." Paper 12 at 14. As the CRU correctly found in its Order Granting Reexamination, Ludtke discloses a "third-party trusted authority" under the PTAB's construction.[1]

[1] Claim terms in a reexam are construed according to the Broadest Reasonable Interpretation of claims, MPEP § 2258(I)(G), while in an IPR, they are

The CRU held that the "third-party trusted authority" is Ludtke's external verification system—its "Access Site"—that verifies a user's "access code" and permits the user to make a phone call. Order at 6.[2] As the CRU recognized, Ludtke discloses a method that uses biometrics to authorize a user seeking to access information services, such as enabling a phone call. *Id.* at 5-6; *see also* Ex. 1005 at Abstract. Ludtke teaches that a user may carry a wireless "transaction device" with a unique identifier. Ex. 1005 at 3:34-35. A user seeking, *e.g.*, to make a phone call may initiate the process using the transaction device. First, the user is required to provide a fingerprint scan to the access device for verification. Order at 6; Ex. 1005 at 18:16-17, 39:54-59. If the fingerprint scan matches an authorized user, a "selection of codes" process follows. *Id.* at 39:47-59. In this selection of codes process, a user inputs an "access code" that is transmitted externally to an "Access Site" for verification. *Id.* at 39:60-40:4. If the access code is verified by Ludtke's Access Site then the user will be permitted to make a phone call. *Id.*

---

construed under the *Phillips* standard. 37 C.F.R. § 42.100(b). Because of this, the Board's construction does not bind the examiner here. *See In re Trans Texas Holdings Corp.*, 498 F.3d 1290, 83 USPQ2d 1835 (Fed. Cir. 2007) (finding prior district court claim construction decision did not bind examiner in later EPR); MPEP 2286 (same). Regardless, and as set forth herein, the claims are unpatentable under the narrower *Phillips* standard and the broader BRI standard.

[2] As used herein, "Order" refers to the CRU's Order Granting Request For *Ex Parte* Reexamination, No. 90/015,053 (November 5, 2022).

The CRU correctly found that this access code verification step at the Access Site discloses "wirelessly sending the ID code for ***comparison by a third-party trusted authority*** [*i.e.*, the Access Site] against one or more previously registered ID codes." Order at 6. Accordingly, Ludtke discloses a "third-party trusted authority" (its "Access Site") under the PTAB's construction, since Ludtke's Access Site is an entity separate from the parties to a transaction (*i.e.*, the caller and the telephone carrier).

PO argues that Ludtke's Access Site cannot be a "third-party trusted authority" because the Access Site ***is*** the system being accessed, and, thus, is not a "third-party" as required by the PTAB's construction. PO Statement at 6-7. PO is incorrect. The "system" being accessed is a ***carrier's telephone network***,[3] not the Access Site itself. The Access Site merely acts as a middleman that grants access to the telephone carrier's service. *Id.* at 40:1-4 ("...Access Site 3250...will ***grant access*** and allow dialing of a call."), 39:41-45 (disclosing accessing, *e.g.*, a "long distance carrier."). Thus, PO's argument that the Access Site is the service being accessed is incorrect.[4]

---

[3] PO admits that "phone company[ies]," not Ludtke's system manage the actual call services. PO Statement at 4.

[4] In addition, PO's argument that the Access Site gives access to ***itself*** based on the verification of a user's access code makes no sense. Ludtke's transaction device is ***already*** in established communication with the Access Site by

But even if Patent Owner's arguments are correct with respect to the CRU's analysis of this term (they are not), PO does not address the disclosure of a "third-party trusted authority" cited in the Reexamination Request. Notably, the Reexamination Request includes another example of a third-party trusted authority: Ludtke's TPCH. PO's Statement fails to address this second example of a "third-party trusted authority."

In particular, as detailed in the Request, Ludtke discloses embodiments in which its system authorizes a transaction with a vendor instead of a phone call. In these embodiments, the transaction device transmits information to a third-party "transaction processing clearing house (TPCH)" for authorization. *Id.* at 3:40-45. This third-party TPCH acts as a middleman between a user and a vendor, blocking a transaction from taking place until verification is complete. *Id.* at 6:36-44, 7:44-46. Thus, this is a second example of a "third-party trusted authority" in Ludtke. Request at 54-56. PO does not dispute that Ludtke's TPCH is a "third-party trusted authority" under the PTAB's construction, leaving Samsung's Request unrebutted in this regard. This provides another independent basis to reject PO's Statement and continue examination.

---

virtue of its transmitting an access code to the Access Site. Thus, the user has access to the Access Site from the outset.

III. LUDTKE DISCLOSES AN "ACCESS MESSAGE"

The challenged claims recite receiving an "***access message*** from the third-party trusted authority" reflecting successful authentication by the third-party trusted authority. This term was not construed by the PTAB. As the CRU correctly found in its Order, Ludtke discloses this limitation.

As explained above, the CRU found that in some embodiments Ludtke teaches an Access Site that grants access to a telephone call. *See* Section II, *supra*. The CRU further found that after access to a telephone network is granted by the Access Site the user receives a dial tone, which is the claimed "access message": "The ***dial tone*** provided to the user becomes an ***access message*** so as to grant access to the dialing of a telephone call." Order at 8 (emphasis added).

PO argues that the "dial tone" in Ludtke cannot be an access message. First, PO argues there is no ID code transmitted in Ludtke, just an "access number." *Id.* at 4. PO argues that Ludtke's "access number" is a telephone phone number. *Id.* PO asserts that Ludtke's access number/phone number is dialed ***before*** the user receives a dial tone from Ludtke's Access Site. *Id.* Thus, PO concludes, Ludtke's "dial tone…is not provided after an ID code ["access number"] is sent to the third-party trusted authority that matches an ID code maintained by the third-party trusted authority" as required by the claims. *Id.*

PO's argument misses the mark. The CRU did not rely on Ludtke's "access number" to show the "ID code" limitation in the first instance. Instead, as discussed above, the CRU relied on Ludtke's teaching of transmitting a user's "***access code***" to Ludtke's Access Site to meet this limitation. Order at 8-9 ("A match of the user's fingerprint at step 3106 then subsequently leads to a ***selection of codes*** at step 3108. In FIG 32 at step 3256, the ***code input is verified externally***. The ***dial tone provided to the user becomes an access message*** so as to grant access to the dialing of the telephone call. ***This generally corresponds to*** 'sends the ID code to a third-party trusted authority for authentication, and that receives ***an access message*** from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code.'") (emphasis added). PO does not dispute that Ludtke's access code is first verified externally at the Access Site, and telephone access is granted after that authentication. A POSITA would understand, as set forth in the attached articles, that during dialing, a "dial tone" indicates "that more dial string characters may be processed," i.e. a call may be placed. Ex. 1016 (RFC 3601) at 4; *see also* Ex. 1017[5](explaining a "dial tone" is part of a handshake protocol designed to establish channel monopoly on Public Switched Telephone Networks to

[5] Analyzing Every Second of the Classic Dial-Up Modem Sound, https://www.popularmechanics.com/science/a29611456/internet-dialup-modem-sounds/.

allow for dialing a call). Thus, Ludtke discloses that its "dial tone" (the claimed "access message") is transmitted only ***after*** the verification step (comparison of the access code to stored codes by the external Access Site). Accordingly, Ludtke's teaches an "access message" even under PO's restrictive understanding of the term.

Even if the CRU had pointed to the "access number" to meet the "ID code" limitation, as PO incorrectly suggests, Ludtke still teaches this claim element. PO itself quotes portions of Ludtke teaching that its access number is dialed before the dial tone is sent:

> ***Initially, the DW…may dial…an access number***…These tones are received at 3252 on the Access Site 3250 side. ***Sometime later a dialtone 3254 is sent*** to the DW 3220 where it is received.

PO Statement at 4, citing Ex. 1005 at 39:63-67. Thus, Ludtke's "access number" (the claimed "ID code") is sent to the Access Site (the claimed "third-party trusted authority") before the dial tone (the claimed "access message") is returned to a user.[6]

Samsung's Request includes an additional example of an access message – an example that PO fails to address. Ludtke expressly teaches that in vendor transactions it is the third-party trusted authority (Ludtke's TPCH) that sends an

[6] In any case, PO's argument that a dial tone is provided ***after*** a telephone number is dialed makes no sense. A telephone number cannot be dialed before there is a dial tone, which reflects an established connection.

indication of approval (the claimed "access message") after the authentication process:

> In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125. In this particular embodiment, a transaction device, e.g., a privacy card 130, is used to maintain the privacy of the user while enabling the user to perform transactions. The ***transaction information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction*** to be performed.

Ex. 1005 at 6:36-44 (emphasis added); Request at 58. Figure 15 also shows this, "TPCH, at step 1520, confirms the transaction and ***provides the confirmation*** to the vendor and the ***user***." Ex 1005 at 27:13-15; Request at 59; *see also* Ex. 1005 Fig. 17, steps 8 and 9-1. This yet another example of an "access message" disclosed in Ludtke. PO does not dispute that this example teaches the claimed "access message." This provides another ground to reject PO's Statement.

IV. CONCLUSION

For the foregoing reasons, the CRU should reject Patent Owner's petition and proceed with *ex parte* reexamination.

DATED: December 8, 2022

Respectfully submitted,

By *__/s/ James M. Glass__*

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan,LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**Certificate of Service**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on December 8, 2022, a copy of the Third Party Requestors Reply to Patent Owner Response, Ex. 1016, and Ex. 1017 were served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
125 Park Avenue, 25th Floor
New York, NY 10017

Dated: December 8, 2022

By: */s/ James M. Glass*
James M. Glass
Reg. No. 46,729

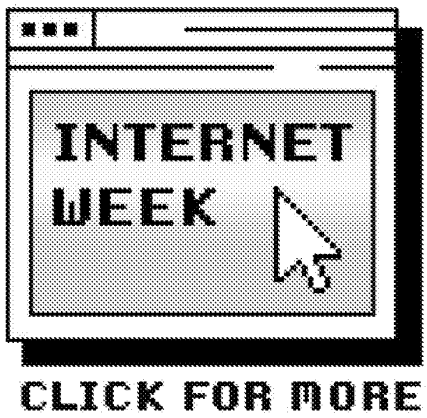
Science > Welcome to Internet Week

Analyzing Every Second of the Classic Dial-Up Modem Sound

Back in the days of dial-up, your computer performed a symphony just to get online. Here's what every bleep, screech, and ding actually did.



BY LYNNE PESKOE-YANG PUBLISHED: MAR 2, 2022

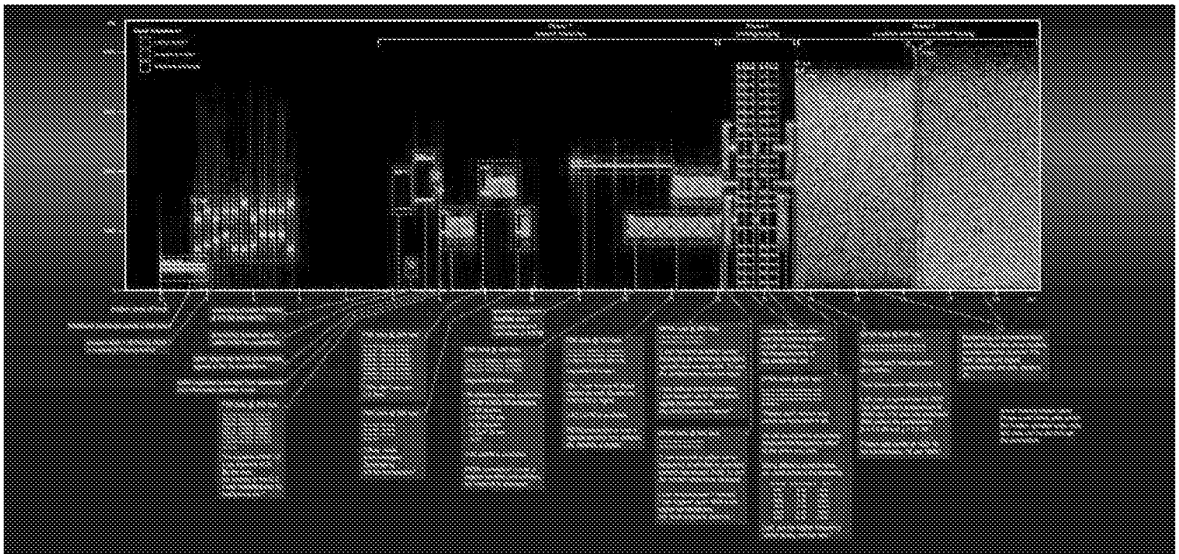


Long before the *vwip!* of iMessage and the funky beats of the Skype startup song, digital communication had a strange soundtrack. Dial-up modems, which connected to servers and other computers via public telephone networks, bracketed the otherwise silent browsing experience with their inimitable song.

But what seemed to internet users to be a noisy side effect of the mystical mechanical process of "going online" actually *was* the process. Known to technicians as a "handshake," the sound was a means of negotiating terms between remote machines, after which they could successfully exchange data during browsing —also with sound, though virtually un-processable to the human ear.

Tech can be tricky. We'll be your support.

The few breakdowns of the mysterious dial-up handshake that remain online invariably include the "example handshake" graphic by Finnish software developer Oona Räisänen below. Räisänen developed the graphic in 2012 to satisfy her own curiosity about the dial-up sound, which was then the subject of a wave of nostalgia for the early days of the commercial internet.



Oona Räisänen, Creative Commons

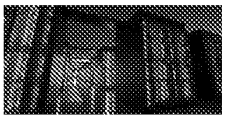
"I had always been intrigued by the fact that computers can literally make phone calls to each other, and I wanted to know exactly how they do that," Räisänen tells *Popular Mechanics*. "I found the information by reading through the ITU-T standards, the technical documents that define different parts of the handshake procedure."

Räisänen discovered that every section of the dial-up song serves a specific purpose: to establish the terms of the coming data transfer for maximal security and minimal information loss. Here, with her help, we break down the iconic sound below, beat by beat.

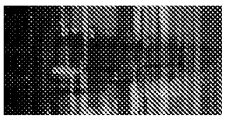
Part 1: Exchanging Pleasantries

The earliest networks, like ARPANET, were limited in reach by their own infrastructure. Dial-up internet was introduced in the early 1990s as a way to work around that obstacle by taking over a signaling system that was already in place worldwide: the Public Switched Telephone Network, or PTSN. The first dial-up modems connected to the internet by using the phone much like humans do: by putting their speakers next to the mouthpiece. Later models could be connected more directly to a building's phone line, though they still took over the phone line completely.

💻 COMPUTER SCIENCE STORIES YOU'LL LOVE



Meet Fugaku, the New Fastest Computer in the World



This Is How Algorithms Will Evolve Themselves



Science Explains Why Hit Songs Sound the Same

That channel monopoly was essential, because the dial-up sound, rather than being a side effect, was the actual conversation between modems; any non-modem audio would just interfere with the signal. "The handshake is not an artifact; it *is* the actual negotiation," writes Räinänen. "All information that the computers exchange is audible in that sound."

Thus the first sound of the handshake is the dial tone, followed by a phone number in the familiar key of Dual-Tone Multi-Frequency, a system that assigns a special tone to every digit, including a country code, area code, and seven-digit phone number. After a pause, the answering modem responds with a tone that initiates a protocol, or a special conversational routine, like V.8bis, another ITU recommendation. When the calling modem accepts the protocol, the real negotiations can begin.

Part 2: Setting the Terms

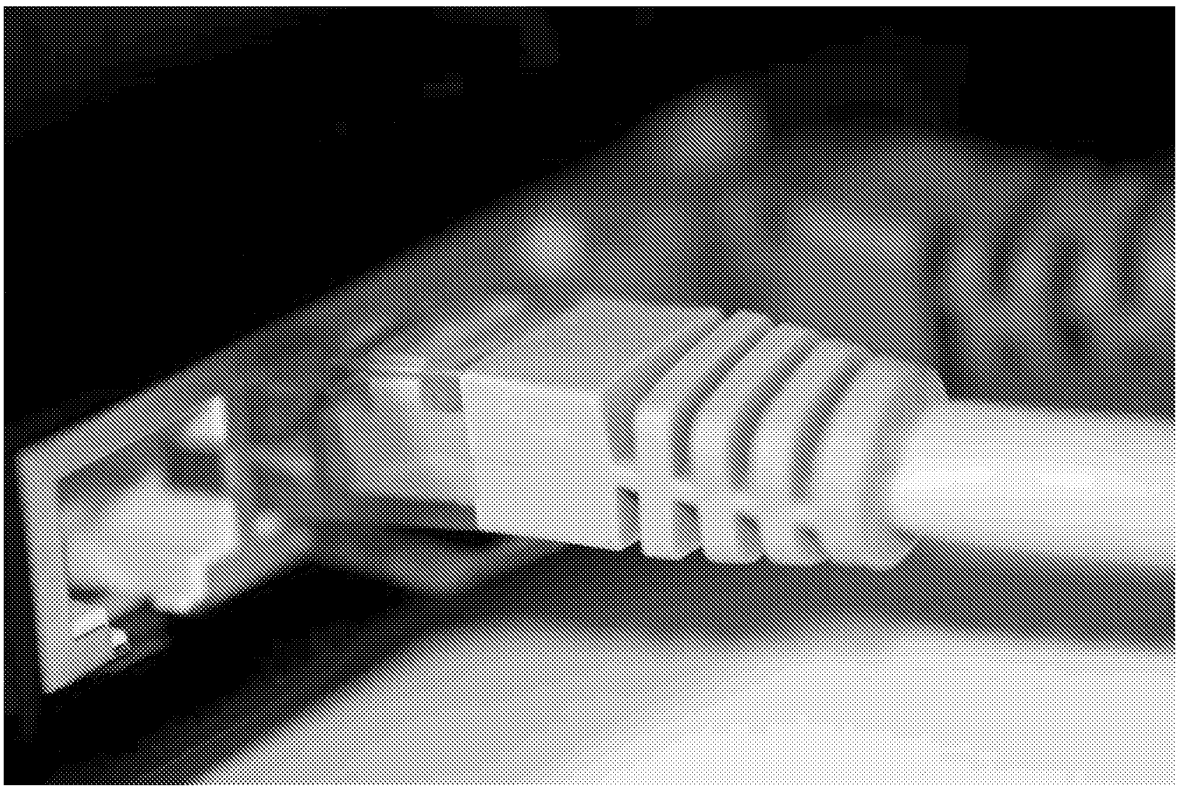
This part of the handshake, in which modems list their capabilities and settle on terms for the connection, really does sound like a conversation. The speakers overlap a little, as conversing humans do, but still leave the impression of a back-and-forth. There's even a bit of a business vibe, albeit what a business would sound like if it were conducted between giant robot-bird-aliens in a screeching tonal shorthand over a busted CB radio.

In the original graphic, Räisanen captures that professional atmosphere by having the modems make requests by saying "please" and sprinkling the translated conversation with chipper exclamation points. "Computer protocols are like extremely rigid rules of etiquette," Räisänen says. "I thought every rule of etiquette should mandate a level of politeness."

Part 3: A Line of Their Own

Hijacking a phone system to connect to the internet requires a lot less hardware than, say, building an international fiber-optic cable network, but dial-up pays a steep price for using borrowed infrastructure. The PSTN offers a few technological features that strongly favor human callers over modems. One of these is echo suppression, which relies on the fact that humans generally take turns speaking on the phone; when one starts talking, the network silences the return channel, which prevents the speaker from being confused by hearing echoes of their own voice.

But modems are full-duplex, which means they have no problem talking and listening at the same time, says Räisänen, so echo suppression just halves the efficiency of the conversation. To eliminate it, the answering modem plays a special tone that disables echo suppression circuit and another circuit modems don't need, called an echo canceller.



Jill Ferry Photography // Getty Images

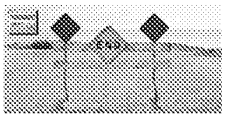
Part 4: Modulation Station

Non-sound information, like bits, doesn't travel happily over sound-only channels like phone lines. It's a classic information theory problem and one of the first topics introduced in digital communications courses. The channel is analog (varying in pitch and volume along the sonic spectrum), but the data are digital (limited to a closed set of symbols like zeroes and ones).

A modem's job is to put one form of information in terms that are legible in the other using one of several protocols that define the unit equivalents between analog and digital data. Turning binary code sequences into analog waveforms—think of the wiggly sound wave you see in audio editing

platforms—is called modulation, and recreating a binary sequence out of a received waveform is demodulation. Modems must perform both processes simultaneously.

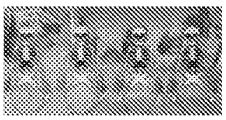
MORE FROM THE INTERNET'S PAST



The Subtle Genius of the 404 Error



How Netscape Won and Then Lost the World Wide Web



The GIF Is Dead. Long Live the GIF.

In order to understand one another, it's essential that the modems use the same key to make their translations, which is why much of the handshake consists of modems chatting about which modes and protocols they prefer. Finding the right modulation mode requires both talking and testing; the modems list the modes they support until they find one they both know, and then emit a series of test tones to figure out which speed will work best over the phone line.

Part 5: Sound Check

At this point, the distinct tones and beeps yield to what sounds like an electric snowstorm that suddenly shifts to a lower pitch before falling silent. The modems have now switched to scrambled data in order to keep the power distribution even across the channel and to weed out any annoying patterns on the line, Räisänen says. More test tones follow in this format; the modems adjust their equalizers to make sure they're not missing any important sounds.

The end of the song comes when modem speakers go silent, allowing the computers themselves to start transferring data according to the terms set during the handshake.

The Evolution of Song

The post dial-up generation of computers relies on its own network infrastructure, satellites, or other wireless transmitters (rather than phone line audio) to connect to the internet, all of which are "hugely faster methods that can't even be expressed as sounds." The most modern routers transmit over specific radio frequencies, bypassing hardware altogether, though they still have to negotiate the way they'll communicate.

"Almost all connections between computers involve some kind of handshake," says Räisänen, but the modern versions "vastly exceed the information capacity of human hearing, or of any sense of biological creature, for that matter."

Robotic communication is now frequently too complex to be understood by humans, including the engineers who design it. Nostalgia for the days of dial-up may be a sign that transparency is almost worth the slowest connection imaginable.



LYNNE PESKOE-YANG

Lynne Peskoe-Yang is a science writer and researcher in New York. Her reporting on civil engineering, machine learning, and artificial intelligence has appeared in *Marketplace*, *IEEE Spectrum*, *Rewire.org*, and *Sludge*; her essays on science and language live over at *Popula*.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan
1300 I Street, Suite 900
Washington, DC 20005

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/015,053* .

PATENT UNDER REEXAMINATION *9298905* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

Order Granting Request For Ex Parte Reexamination	Control No. 90/015,053	Patent Under Reexamination 9298905	
	Examiner SAM RIMELL	Art Unit 3992	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed 06/08/2022 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☑ PTO/SB/08, c)☐ Other: ____

1. ☑ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

cc:Requester (if third party requester)

DECISION GRANTING EX PARTE REEXAMINATION

The Request filed June 8, 2022 alleges that substantial questions of patentability (SNQ) affecting claims 1-18 of the U.S. Patent Number 9,298,905 are raised by the following prior art references:

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Brief Overview of US Patent 9,298,905

The invention pertains to systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

Prosecution History of US Patent 9,298,905

US Patent 9,298,905 resulted from the filing of US application 14/521,982 filed October 23, 2014, with a priority claim extending to provisional application 60/637,538 filed December 20, 2004.

The USPTO mailed a non-final office action on June 12, 2015. Claims 11 and 15 were rejected under the provisions of non-statutory double patenting. Claims 2-10 were rejected under 35 USC §101. Claims 2-10 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126). Claims 3 and 13 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126) and Schlotterbeck (US Pre-Grant Publication 2004/0128162). Claims 11-12 and 14-18 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126) and Lake (US Pre-Grant publication 2002/0091646).

On September 14, 2015, applicant submitted aa reply with amendments and remarks.

On December 16, 2015, the USPTO issued a Notice of Allowance with claims 2-7 and 9-20 allowed and claims 1 and 8 cancelled. These were subsequently re-numbered as claims 1-18.

The reasons for patentability read as follows:

"The closest prior arts cited are generally directed to various aspects of authenticating users using biometric information. However, none of the cited arts found alone or in combination suggests or teaches all the elements of the independent claims. For instance, no parts of the cited arts teach or suggest limitations such as persistently storing biometric data of a legitimate user and an ID code on an integrated device; responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor; comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third- party

trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction. Therefore, the claims are allowable for the above reason."

Inter Partes Review before Patent Trial and Appeal Board

The records of the Patent Trial and Appeal Board contain the following *Inter Partes* Review Proceedings involving claims of US Patent 9,298,905:

AIA Review #	Filing Date	Institution Decision Date	Petitioner App #	Petitioner Patent #	Petitioner Tech Center	Petitioner	PO/Respondent App #	PO/Respondent Patent #	PO/Respondent Tech Center	PO/Respondent	Status
IPR2021-01447	09/26/2021	03/28/2022				SAMSUNG ELECTRONICS AMERICA, INC	14521982	9298905	2400	Proxense, LLC	Institution Denied

Final Decisions in the Federal Circuit

There are no known final decisions in the Federal Circuit involving US Patent 9,298,905.

Applicability of "Old Art" in Reexamination Proceedings

In the examining stage of a reexamination proceeding, the examiner will consider whether the claims are subject to rejection based on art. Before making such a rejection, the examiner should check the patent's file history to ascertain whether the art that will provide the basis for the rejection was previously cited/considered in an earlier concluded Office examination of the patent (e.g., in the examination of the application for the patent). For the sake of expediency, such art is referred to as "old art" throughout, since the term "old art" was coined by the Federal Circuit in its decision of *In re Hiniker*, 150 F.3d 1362, 1365-66, 47 USPQ2d 1523, 1526 (Fed. Cir. 1998).

If the rejection to be made by the examiner will be based on a combination of "old art" and art newly cited during the reexamination proceeding, the rejection is proper, and should be made.

See *In re Hiniker*, 150 F.3d at 1367, 47 USPQ2d at 1527. (Court held the reexamination proceeding was supported by a substantial new question of patentability where the rejection before the court was based on a combination of art that had been before the examiner during the original prosecution, and art newly cited during the reexamination proceeding.)

For a reexamination that was ordered on or after November 2, 2002 (the date of enactment of Public Law 107-273; see Section 13105, of the Patent and Trademark Office Authorization Act of 2002), reliance solely on old art (as the basis for a rejection) does not necessarily preclude the existence of a substantial new question of patentability (SNQ) that is based exclusively on that old art. Determinations on whether a SNQ exists in such an instance shall be based upon a fact-specific inquiry done on a case-by-case basis. For example, a SNQ may be based solely on old art where the old art is being presented/viewed in a new light, or in a different way, as compared with its use in the earlier concluded examination(s), in view of a material new argument or interpretation presented in the request.

Discussion of SNQs

Issue #1

Requester proposes that Ludtke in view of Okereke raise a substantial new question of patentability (SNQ) with respect to claims 1, 3-10 and 12-18. From this claim set, claims 1, 9, and 13 are the independent claims.

Independent claim 1 recites:

"*receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor; comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; responsive to a determination that the scan data matches the*

biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes"

Ludtke at col. 4, line 66 through col. 5, line 1, states "Alternately, authentication may be achieved by using more sophisticated technologies such as a biometric solution (e.g. fingerprint recognition)". This generally corresponds to "*receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor*". Ludtke at col. 14, lines 33-36 recite: "The user authentication block 777 preferably includes a biometric solution of validating that the user interacting with the device is an authorized user. This can be achieved, for example, by using a fingerprint recognition pad." Ludtke at col. 14, lines 40-46 further recite: "At various times during interaction, the user is prompted to supply a fingerprint recognition sample. This block captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block described above. If a match is found, the user is authorized to access the data and functionality of the device." These features generally correspond to "*comparing the scan data to the biometric data to determine whether the scan data matches the biometric data*". Ludtke at FIG 31 illustrates the financial transaction process where steps 3104, 3106 and 3110 involve processing of the user's fingerprint. A match of the user's fingerprint at step 3106 then subsequently leads to a selection of codes at step 3108. In FIG 32 at step 3256, the code input is verified to grant access to the dialing of a telephone call. Ludtke at col. 15, lines 7-12 indicate that data input functions can be performed wirelessly. This generally corresponds to "*wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes*"

Independent claim 9 recites:

"*a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority*"

Ludtke at FIG 7C teaches a user authentication module 777 which is integrated with persistent memory storage, as illustrated by the memory/info stick of FIG 9B. This generally corresponds to "*a validation module, coupled to communicate with the persistent storage media*". Ludtke at col. 14, lines 33-36 recite: "The user authentication block 777 preferably includes a biometric solution of validating that the user interacting with the device is an authorized user. This can be achieved, for example, by using a fingerprint recognition pad." Ludtke at col. 14, lines 40-46 further recite: "At various times during interaction, the user is prompted to supply a fingerprint recognition sample. This block captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block described above. If a match is found, the user is authorized to access the data and functionality of the device." These features generally correspond to "*receives scan data from a biometric scan for comparison against the biometric data*". Ludtke at FIG 31 illustrates the financial transaction process where steps 3104, 3106 and 3110 involve processing of the user's fingerprint. A match of the user's fingerprint at step 3106 then subsequently leads to a selection of codes at step 3108. In FIG 32 at step 3256, the code input is verified externally to grant access to the dialing of a telephone call. This generally corresponds to *sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority*".

Independent claim 13 recites:

"*an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code*".

Ludtke at FIG 7C teaches hardware component 777 which is integrated with persistent memory storage, as illustrated by the memory/info stick of FIG 9B. This generally corresponds to "*an integrated hardware device that persistently stores biometric data of a legitimate user*". Ludtke at FIG 7B also teaches a smart chip interface, which generally correspond to "*an ID code in the integrated hardware device*". Ludtke at col. 15, lines 7-12 indicate that data input functions can be performed wirelessly. This generally corresponds to "*wirelessly sending the ID code*".

Ludtke at col. 14, lines 40-46 further recite: "At various times during interaction, the user is prompted to supply a fingerprint recognition sample. This block captures the sample, and carries out a recognition algorithm against the authorized samples that are stored in the user identity block described above. If a match is found, the user is authorized to access the data and functionality of the device." These features generally correspond to "*an authentication circuit that receives the ED code*".

Ludtke at FIG 31 illustrates the financial transaction process where steps 3104, 3106 and 3110 involve processing of the user's fingerprint. A match of the user's fingerprint at step 3106 then subsequently leads to a selection of codes at step 3108. In FIG 32 at step 3256, the code input is verified externally. The dial tone provided to the user becomes an access message so as to to grant access to the dialing of a telephone call. This generally corresponds to "*sends the ID code to*

a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code".

There is a substantial likelihood that a reasonable examiner would consider these teachings of Ludtke important in deciding the patentability of independent claims 1, 9, and 13. The reference to Ludtke is not cumulative to the prior art of record in the original file and the claim was not subject to a final holding of invalidity by a federal court. Accordingly, Ludtke raises a substantial new question of patentability with respect to claims 1, 9 and 13.

Since dependent claims 3-8, 10, 12 and 14-18 would incorporate the language of the independent claims by reference, the reference to Ludtke would equally raise a substantial new question of patentability with respect to the dependent claims 3-8, 10, 12 and 14-18.

A combination of prior art including the Ludtke reference, such as Ludtke and Okereke would further raise a substantial new question of patentability with respect to claims 1, 3-10 and 12-18, since the combination would at least include the teachings of Ludtke.

Issue #2

Requester proposes that Ludtke in view of Okereke and Robinson raise a substantial new question of patentability (SNQ) with respect to dependent claims 2 and 11.

Ludtke was established in Issue #1 as raising an SNQ with respect to all of the independent claims 1, 9 and 13. Since dependent claims 2 and 11 would incorporate the language of the independent claims by reference, the reference to Ludtke would equally raise a substantial new question of patentability with respect to the dependent claims 2 and 11.

A combination of prior art including the Ludtke reference, such as Ludtke in view of Okereke and Robinson, would further raise a substantial new question of patentability with respect to claims 2 and 11, since the combination would at least include the teachings of Ludtke.

Issue #3

Requester proposes that Ludtke in view of Scott raise a substantial new question of patentability (SNQ) with respect to claims 1, 3-10 and 12-18.

Ludtke was established in Issue #1 as raising an SNQ with respect to all of the independent claims 1, 9 and 13. Since dependent claims 3-8, 10, 12 and 14-18 would incorporate the language of the independent claims by reference, the reference to Ludtke would equally raise a substantial new question of patentability with respect to the dependent claims 3-8, 10, 12 and 14-18.

A combination of prior art including the Ludtke reference, such as Ludtke in view of Scott, would further raise a substantial new question of patentability with respect to claims1 , 3-10 and 12-18 since the combination would at least include the teachings of Ludtke.

Issue #4

Requester proposes that Ludtke in view of Scott and Robinson raise a substantial new question of patentability (SNQ) with respect to dependent claims 2 and 11.

Ludtke was established in Issue #1 as raising an SNQ with respect to all of the independent claims 1, 9 and 13. Since dependent claims 2 and 11 would incorporate the language of the independent claims by reference, the reference to Ludtke would equally raise a substantial new question of patentability with respect to the dependent claims 2 and 11.

A combination of prior art including the Ludtke reference, such as Ludtke in view of Scott and Robinson, would further raise a substantial new question of patentability with respect to claims 2 and 11, since the combination would at least include the teachings of Ludtke.

Summary of Findings

Issues	References	Substantial New Question of Patentability with respect to claims of US Patent 6,212,662
#1	Ludtke, Okereke	Claims 1, 3-10, 12-18: Yes
#2	Ludtke, Okereke, Robinson	Claims 2, 11: Yes
#3	Ludtke, Scott	Claims 1, 3-10, 12-18 : Yes
#4	Ludtke, Scott, Robinson	Claim 2, 11: Yes

35 USC 325(d)

A review of the post grant history for the '905 Patent indicates that a single AIA post grant challenge has been filed. On August 26, 2021, SAMSUNG ELECTRONICS AMERICA, INC. filed a petition for *inter partes* review (IPR2021-01447) asserting a reasonable likelihood in prevailing (RLP) in showing the unpatentability of claims 1-12 of the '905 Patent. The petition asserted that claims 1-9 were unpatentable under 103(a) over Scott and Lapsley (Ground #1), unpatentable under 103(a) over Scott, Lapsley and Robinson (Ground #2) and unpatentable under 103(a) over Berardi, Shreve and Kinoshita (Ground #3). On February, 28, 2022, the Board issued a decision denying the petition as not raising an RLP to any of the challenged claims.

In the Board's decision refusion to institute *inter partes* review, regarding Grounds #1 and #2, the Board held that "Petitioner does not show persuasively that either Scott or Lapsley teaches a "third-party trusted authority," as recited in claim 1… or that (IPR2021-01447, pages 25 and 26). Regarding Ground #3, the Board held that "we cannot discern Petitioner's allegations of obviousness based on Berardi, Shreve, and Kinoshita, nor can we say Patent Owner is on

notice of those allegations (IPR202-10447 pages 30). Thus, the Board that the petition failed to raise an RLP for any of three asserted grounds in the petition.

A review of the AIA petition as compared to the instant request for *ex parte* reexamination indicates both the Scott and Robinson prior art references that were presented in the prior AIA petition are also being presented in the instant reexamination request also filed by Samsung (See SNQs #2, #3 and #4). However even though Scott was used in the prior AIA petition, they are now being used as a part of a different grounds of rejection as secondary references with the newly presented Luedtke as a primary reference (See proposed SNQ #2 #3 and #4). Further, the request specifically presents newly cited Ludtke to address the omission identified as the basis for the Board's refusal to institute in IPR2021-01447. As pointed out by third party requester, Ludtke specifically discloses a transaction processing [or privacy] clearing house (TCPH) which is a third-party trusted authority, and further discloses that the TPCH "may access relevant account information to authorize transactions." See Col. 3:40-45. Thus, the teachings cited to in Lutke and arguments related to Lutke presented in the instant reexamination request were not present in the prior AIA petition and relate to limitations the Board held was not present in Scott. Accordingly, the prior art and arguments provided in the request are not the same or substantially the same as those presented IPR2021-01447.

Accordingly, in view of the above facts, particularly the fact that the request is not based on substantially the same prior art or arguments, a discretionary denial of reexamination pursuant to 35 USC 325(d) is not implicated and reexamination will be Ordered for the reasons set forth above.

Service of Papers

After filing of a request for ex parte reexamination by a third party requester, any document filed by either the patent owner or the third party requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR 1.248. The document must reflect service or the document may be refused consideration by the Office. See 37 CFR 1.550(f).

Extensions of Time

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

Litigation Reminder

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving US Patent 9,298,905 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

All correspondence relating to this *ex parte* reexamination proceeding should be directed as follows:

By **U.S. Postal Service Mail** to:

Mail Stop *Ex Parte* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents

P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand to: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Reexamination Legal Advisor or Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/SAMUEL G RIMELL/
Primary Examiner, Art Unit 3992

Conferees:

/JDC/ Jeff Carlson
Primary Examiner, Art Unit 3992

/MICHAEL FUELLING/
Supervisory Patent Examiner, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/015,053	9298905
	Examiner	Art Unit
	SAM RIMELL	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Reviewed US Patent 9,298,905 and prosecution history	07/29/2022	SR
Reviewed PTAB E2E system for any IP proceedings related to US 9,298,905. Found one: IPR 2021-01447 (institution denied)	07/29/2022	SR

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/015,053	9298905
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
Marissa Ducca Quinn Emanuel Urquhart & Sullivan 1300 I Street NW Suite 900 Washington, DC 20005

LITIGATION REVIEW ☐	SR (examiner initials)	29 July 2022 (date)
Case Name		Director Initials
None		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

PTO/SB/08a (07-09)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	14/521,982
Filing Date	October 23, 2014
First Named Inventor	John J. Giobbi
Art Unit	
Examiner Name	
Attorney Docket Number	

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number / Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/S.G.R/		US- 7,188,110 B1	03-06-2007	Ludtke	
/S.G.R/		US- 2003/0196084 A1	10-16-2003	Okereke	
/S.G.R/		US- 2003/0177102 A1	09-18-2003	Robinson	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document / Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
/S.G.R/		WO 1999/056429 A1	11-04-1999	Scott		

Examiner Signature	/SAMUEL G RIMELL/	Date Considered	07/29/2022

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0031. Public burden for this form is estimated to average 2 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. If** filing this completed form by mail, send to: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a Federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 9) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Additional Uses

Additional USPTO uses of the information in this record may include disclosure to: 1) the International Bureau of the World Intellectual Property Organization, if the record is related to an international application filed under the Patent Cooperation Treaty; 2) the public i) after publication of the application pursuant to 35 U.S.C. 122(b), ii) after issuance of a patent pursuant to 35 U.S.C. 151, iii) if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections, or an issued patent, or iv) without publication of the application or patent under the specific circumstances provided for by 37 CFR 1.14(a)(1)(v)-(vii); and/or 3) the National Archives and Records Administration, for inspection of records.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi		Examiner:	Rimell, Samuel G
U.S. Patent No.:	9,298,905	Art Unit:	3992
Issued:	March 29, 2016		
Application No.:	14/521,982		
Filed:	October 23, 2014		
Title:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION		

PATENT OWNER RESPONSE

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Commissioner:

Proxense, the owner of U.S. Patent 9,298,905 ("905 Patent") hereby responds to the *Ex Parte* Reexamination Petition filed by Samsung Electronics America, Inc. ("Samsung"). For the reasons described herein, these Reexamination proceedings should be terminated.

TABLE OF CONTENTS

I. The Prior Art Does Not (Alone or in Combination) Include an "Access Message" or "Third-Party Trusted Authority" 3

A. *Ludtke*'s Dial Tone is Not an "Access Message" 4

B. *Okereke and Robinson* Do Not Disclose an "Access Message" 5

II. Construction of "Third-Party Trusted Authority" 5

III. The Prior Art (Alone or in Combination) Does Not Include a "Third-Party Trusted Authority" 6

IV. Conclusion 7

Pursuant to 37 CFR 1.530 and 35 U.S.C. 304, Patent Owner respectfully submits this patent owner statement.

At bottom, the patent claims of U.S. Patent No. 9,298,905 are patentable considering the cited prior art patents and printed publications alone or in any reasonable combination. Specifically, none of the prior art discloses either an "access message" or "third-party trusted authority," as that term has been construed by the Patent Trial and Appeal Board ("PTAB").

I. THE PRIOR ART DOES NOT (ALONE OR IN COMBINATION) INCLUDE AN "ACCESS MESSAGE" OR "THIRD-PARTY TRUSTED AUTHORITY"

The substantial new questions of patentability identified by the Examiner do not to establish the presence of an access message as defined by the claims. Claims 1, 9 and 13 recites receipt of "an access message … indicating that the ***third-party trusted authority successfully authenticated the ID code.***" Claims 1 and 9 require that the ID code be "one or more previously registered ID codes ***maintained by the third-party trusted authority***."

Similarly, claim 13 requires the ID code be one of a list of legitimate codes maintained by the third-party trusted authority in recite "the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received ***based on a comparison of the ID code received and the legitimate codes including in the list of the legitimate codes***". As the access message indicates the third-party trusted authority "successfully authenticated the ID code" and the third-party trusted authority maintains legitimate or previously registered ID codes, the access message is only received after an ID code is sent to the third-party trusted authority that matches an ID code maintained by the third-party trusted authority. Accordingly, the substantial new questions of patentability identified by the Examiner do not establish the presence of such an access message in the prior art.

A. *Ludtke*'s Dial Tone is Not an "Access Message"

In identifying a substantial new question of patentability, the Examiner states "the dial tone provided to the user becomes an access message". *Decision on Request for Ex Parte Reexamination,* mailed August 2, 2022, at 8. The dial tone, however, is not provided after an ID code is sent to the third-party trusted authority that matches an ID code maintained by the third-party trusted authority. As explained by *Ludtke* (U.S. Patent No. 7,188,110), "Initially, the DW at 3222 may **dial**, for example via tones, **an access number** and wait a number of seconds. These tones are received at 3252 on the Access Site 3250 side. Sometime later a dialtone 3254 is sent to the DW 3220 where it is received." *Ludtke,* 39:63-67. Dialing an access number is placing phone a call; the disclosed "access number" is not the same as the disclosed "access code," which is used after the phone call is placed using the "access number." In other words, the DW is dialing the phone number of the access site before it receives the dialtone. A phone number is not an ID code. The claims require that the ID code be maintained by the third-party trusted authority. *Ludtke* nowhere discloses that the **access number** is maintained by the third-party trusted authority. Nor could it. Phone numbers, after all, are maintained by the phone company issuing them, not the person or entity possessing them. As such, the access number (*i.e.*, phone number of the access site 3250) in *Ludtke* is not an ID code as recited in the claims.

Furthermore, the dial tone is sent sometime after the DW 3220 dials the access number. *Ludtke* thus discloses the dial is sent in response to dialing a phone number. The claims, however, require the access message be received only after an ID code is sent to the third-party trusted authority. Since a phone number is not the claimed ID code, the dial tone is not received after sending an ID code as claimed. Consequently, the dial tone is not an "access message" as defined by the claims.

B. *Okereke and Robinson* Do Not Disclose an "Access Message"

The Examiner has not pointed to the teachings of *Okereke* (U.S. Publication No. 2003/0196084) or *Robinson* (U.S. Publication No. 2003/0177102) as raising substantial new questions of patentability with respect to an access message. With regards to *Scott* (International Publication No. WO 99/56429), the PTAB has already determined *Scott* fails to disclose an access message. *Samsung Electronics America, Inc. v. Proxense, LLC,* IPR2021-01447, Paper 12 at 25-26 (PTAB February 28, 2022). The substantial new questions of patentability identified by the Examiner do not establish questions regarding an access message, and do not address all the limitations of the claims.

II. CONSTRUCTION OF "THIRD-PARTY TRUSTED AUTHORITY"

In addition to failing to demonstrate questions regarding an access message as defined by the claims, the substantial new questions of patentability fail to establish regarding a third-party trusted authority. "During reexamination ordered under 35 U.S.C. § 304 … claims are given the broadest reasonable interpretation consistent with the specification". MPEP § 2258(I)G). "Under a broadest reasonable interpretation (BRI), words of the claim must be given their plain meaning, unless such meaning is inconsistent with the specification". MPEP § 2111.01(I). Accordingly, during reexamination, terms of the claim are typically given their plain meaning. With respect to the '905 Patent, the Patent Trial and Appeal Board ("PTAB") has already ruled as to the plain meaning of "third-party trusted authority" and thus decided the broadest reasonable interpretation of the claims.

In particular, the PTAB found that "[t]he plain meaning of 'third-party trusted authority' suggests an entity or party separate from the principal parties to a transaction". IPR2021-01447, Paper 12 at 13. The PTAB further noted such was consistent with specification – noting Figure 3 "depicts trusted key authority 320 as an entity separate from biometric key 100, authentication

module 310, and application 330". *Id.* Accordingly, the PTAB interpreted the plain meaning of "third-party trusted authority" consistent with the specification to be "a trusted authority that is an entity separate from the parties to a transaction". *Id,* 14. As the plain meaning defines the broadest reasonable interpretation consistent with the specification, the PTAB has already determined the broadest reasonable interpretation of "third-party trusted authority" and, therefore, the construction of the term to be applied in this reexamination.

The PTAB has also determined how the broadest reasonable interpretation of "third-party trusted authority" is to be applied when evaluating prior art. When distinguishing claim 1 from the prior art, the PTAB noted "the DPC appears to be what is being accessed, as the payee and payor, with the PIA, access a list of financial accounts from the DPC. Here, the DPC is the resource to be accessed, but it is a party to the transaction, rather than a third-party". *Id, at* 24 (internal citations omitted). Accordingly, under the broadest reasonable interpretation, a third-party trusted cannot be what is being accessed. The purported substantial new questions of patentability identified fail to account for a third-party trusted authority as the PTAB has defined it (consistent with the broadest reasonable interpretation), which cannot be the system being accessed.

III. THE PRIOR ART (ALONE OR IN COMBINATION) DOES NOT INCLUDE A "THIRD-PARTY TRUSTED AUTHORITY"

Each of the independent claims at issue require communicating with a third-party trusted authority that, under the broadest reasonable interpretation, is not the system being accessed. In finding substantial new questions of patentability, the Examiner identified the access site 3250 of *Ludtke* as the third-party trusted authority. *Ludtke,* however, states access site 3250 "will grant access and allow dialing of a call." *Ludtke,* 40:3-4. By granting access and allowing dialing of a call the access site 3250 of *Ludtke* is the system being accessed to place call. The PTAB has

already determined the broadest reasonable interpretation of "third-party trusted authority", under which a third-party trusted not the system being accessed. Thus, because *Ludtke's* access site 3250 is the system being accessed to place a call, it is not a third-party trusted authority under what the Boards has determined to be the broadest reasonable interpretation.

The Examiner has not pointed any teachings of *Okereke* or *Robinson* as raising substantial new questions of patentability with respect to a third-party trusted authority.

With regards to *Scott* (International Publication No. WO 99/56429), the PTAB specifically held *Scott* fails to disclose a third-party trusted authority. IPR2021-01447, Paper 12 at 22. In view of this determination, it cannot be found that *Scott* discloses a third-party trusted authority as recited in the claims.

IV. CONCLUSION

In view of the foregoing, the substantial new questions of patentability identified by the Examiner do not establish questions regarding an access message and third-party trusted authority components, and thus do not address all the limitations of the claims. In addition to not addressing all the limitations of the claims, the substantial new questions of patentability do not demonstrate the claims at issue are either anticipated or rendered obvious by *Ludtke, Okereke,* or *Scott,* alone or in combination. Termination of these proceedings, therefore, is respectfully requested.

DATED: November 2, 2022

Respectfully Submitted,

Hard IP LLC

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598
Email: kinza@hard-ip.net

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. PATENT NO.:	9,298,905	ART UNIT:	3992
CONTROL NUMBER:	90/015,053	CONF. NO.:	7424
FILING DATE:	October 23, 2014	EXAMINER:	RIMELL, SAMUEL G.

TITLE: **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

FILED ELECTRONICALLY

Mail Stop *Ex Parte* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF SERVICE ON THIRD-PARTY REQUESTOR

Dear Commissioner:

The undersigned, on behalf of the Patent Owner, hereby certifies that a copy of the following document is being served on the Third-Party Requestor by first class mail on November 2, 2022:

1. Patent Owner Response

The name and addresses of the parties being served are as follows:

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005

Attorneys for Third-Party Requestor, Samsung Electronics America, Inc.

Respectfully submitted,

Hard IP LLC

Dated: November 2, 2022

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598
Email: kinza@hard-ip.net

Electronic Acknowledgement Receipt	
EFS ID:	46948750
Application Number:	90015053
International Application Number:	
Confirmation Number:	7424
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	9298905
Customer Number:	142179
Filer:	Kinza Hecht/Eddie Rowell
Filer Authorized By:	Kinza Hecht
Attorney Docket Number:	2090-0002-REX
Receipt Date:	02-NOV-2022
Filing Date:	08-JUN-2022
Time Stamp:	19:30:37
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Timely Patent Owner's Stmnt in Resp to Order	2090_0002-REX_905_Resp.pdf	124909 a1685330937c5fb029ddc39e25c8fce956c535f4	no	7

Warnings:

Information:					
2	Reexam Certificate of Service	1-905_Certificate_of_Service.pdf	25563 5b9307b374dc250a2f5d51489ee5bce24309b761	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	150472	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/015,053	**10/04/2022 01:36:36 PM ET**	**2090-0002-REX**

Title of Invention

Biometric personal data key (PDK) authentication

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	9298905
CONFIRMATION #	7424	FILED BY	James Glass
PATENT CENTER #	61031921	FILING DATE	06/08/2022
CUSTOMER #	142179	FIRST NAMED INVENTOR	- 9298905
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Opp to Second EPR Pet - 905___.pdf	19	Reexam - Opposition filed in response to petition	270 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Opp to Second EPR Pet - 905___.pdf	A1021F60E0ED1CA5E0FF31DB1071E0FF8688AFFAEDCEAD04 A1F342E0512B0F765B8F6DA7C1143D231E04395FE18652EA2C 1BA189FBE334CAE1C98148C5E4C961

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as

described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: Rimell, Samuel G.
Issued: March 29, 2016	Art Unit: 3992
Application No.: 14/521,982	
FiledOctober 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**RESPONSE TO PATENT OWNER'S (SECOND) PETITION UNDER 1.181(A)(2)**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Samsung Electronics America, Inc. ("Samsung" or "Requestor") hereby responds to Patent Owner's second petition under 37 C.F.R. § 1.181 requesting termination of the above-captioned *ex parte* reexamination of claims 1-18 (the "Challenged Claims") of U.S. Patent No. 9,298,905 ("the '989 patent"). For the reasons described herein, Patent Owner's second petition should be denied.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. PATENT OWNER FILED ITS SECOND PETITION WITHOUT CRU AUTHORIZATION 2

III. *IN RE VIVINT* DOES NOT PRECLUDE SAMSUNG'S REQUEST FOR *EX PARTE* REEXAMINATION 4

IV. ROADMAPPING CONCERNS DO NOT APPLY TO SAMSUNG'S REQUEST 6

V. DENIAL OF INSTITUTION BASED ON § 325(D) IS NOT WARRANTED 7

A. Patent Owner's Petition Relies On The Wrong Legal Standard 7

1. GP Factor 1: Whether The Same Petitioner Previously Filed A Petition Directed To The Same Claims Of The Same Patent 9

2. GP Factor 2: Whether At The Time Of Filing Of The First Petition The Petitioner Knew Of The Prior Art Asserted In The Second Petition Or Should Have Known Of It 10

3. GP Factor 3: Whether At The Time Of Filing Of The Request For Reexamination The Requestor Already Received The Patent Owner's Preliminary Response To The previous IPR Petition Or Received The Board's Decision On Whether To Institute Review 11

4. GP Factor 4: The Length Of Time That Elapsed Between The Time The Petitioner Learned Of The Prior Art Asserted In The Second Petition And The Filing Of The Second Petition 11

5. GP Factor 5: Whether The Petitioner Provides Adequate Explanation For The Time Elapsed Between The Filings Of Multiple Petitions Directed To The Same Claims Of The Same Patent 12

6. GP Factor 6: The Finite Resources Of The Board 12

7. GP Factor 7: The Requirement For The PTAB To Issue A Final Determination No Later Than 1 Year After The Date On Which The Director Notices Institution Of Review....13

VI. THE DIRECTOR SHOULD INVOKE HER OWN INITIATIVE UNDER 35 U.S.C. § 303(A)....14

VII. CONCLUSION....14

I. INTRODUCTION

As the Central Reexamination Unit ("CRU") has already correctly found, "discretionary denial pursuant to 35 U.S.C § 325(d) is not implicated" here, because the instant reexamination request is not a serial filing, and because Samsung's request presents substantial new questions of patentability ("SNQ") not cumulative of art or arguments previously presented before the PTO. Order at 12.[1] Patent Owner's second petition should be rejected for the same reasons.

Moreover, Patent Owner's second petition should be denied as procedurally improper. The CRU did not give Patent Owner permission to file a second petition, let alone file a reply addressing the arguments made in Samsung's opposition. The rules do not authorize any such additional briefing, and, in any case, Patent Owner cites no reason why it could not have included its new arguments in its initial petition. *See* 37 C.F.R. § 1.181. Accordingly, Patent Owner's petition should be rejected.

Even if the CRU grants entry of Patent Owner's second petition, the petition should be denied because it fails to address the correct legal standard. In particular, Patent Owner seeks relief under Section 325(d), but the petition includes a (modified) analysis of Section 314(a). Patent Owner cites no precedent that a

[1] CRU Order Granting Request For Reexamination (August 2, 2022) (hereinafter, "Order").

Section 314(a) analysis applies to petitions to terminate already-instituted reexam proceedings, let alone that it replaces the required analysis for petitions filed pursuant to Section 325(d). For all of these reasons, the CRU should deny Patent Owner's second petition.

II. PATENT OWNER FILED ITS SECOND PETITION WITHOUT CRU AUTHORIZATION

On July 28, 2022, the CRU issued a decision granting entry of Patent Owner's initial Section 325(d) petition. *See* App. No. 90/015,053, Decision On 37 CFR 1.183 Petition at 2 (July 28, 2022) (the "Decision"). In its Decision, the CRU expressly denied Patent Owner's request for waiver of the rules to file a second petition, finding that the request for a second petition was "premature." *Id.* at 3 ("Patent owner's request for waiver of the rules to permit the Office to enter and consider a future petition directed to issues under § 325(d) is **premature**.") (emphasis in original). Thus, the CRU's Decision denied Patent Owner's request to file a second petition.

The CRU's Decision also mandated that any future request to file a second petition must include a request under 37 CFR 1.183 for waiver of the applicable rules. *Id.* at n. 5.

Ignoring the CRU's directives, Patent Owner filed a second petition under § 1.181 without seeking permission from the CRU and without including a request for waiver under 37 CFR 1.183 as the CRU instructed.

Patent Owner's second petition should be denied as procedurally improper because it was filed without CRU authorization and in contravention of the CRU's directives. Indeed, granting entry of Patent Owner's second petition would set a dangerous precedent that parties can ignore directives from the CRU and file follow-on briefing without authorization or justification. This is especially true where, as here, Patent Owner has failed to explain why its arguments could not have been included in its initial petition, let alone show that good cause exists requiring a second petition.

Moreover, Patent Owner has not cited any authority (in either of its two petitions) that permits it to file a what is effectively a reply brief, filling gaps in its initial petition and addressing arguments made in Samsung's opposition. The statute does not permit such a filing. *See* 37 C.F.R. § 1.181. Nothing in the language of the statute suggests multiple rounds of briefing is permitted. *Id.* Accordingly, Patent Owner's petition should be denied on procedural grounds.

III. *IN RE VIVINT* DOES NOT PRECLUDE SAMSUNG'S REQUEST FOR *EX PARTE* REEXAMINATION

Even if Patent Owner's second petition is granted entry for consideration, it should be rejected on the merits. Patent Owner's petition rests on the erroneous assumption that *In re Vivint* categorically precludes *ex parte* reexamination where an IPR petition was previously filed. This is not the law.

In re Vivint does not stand for the proposition that a requestor is precluded from filing an *ex parte* reexamination request where a single IPR petition was denied earlier. Instead, as discussed in Samsung's initial opposition, *In re Vivint* addressed an egregious case wherein a requestor had already filed ***three*** "undesirable, incremental" petitions (all of which were denied). *See In re Vivint, Inc.* 14 F.4th 1342 at 1346 (Fed. Cir. 2021). That is not the case here.

Further, in *In re Vivint* the Board effectively relied upon its discretionary authority under Section 325(d) as the basis for its denial of the last serial IPR petition. *Id.* at 1353 (finding that Board "actually relied on § 325(d) considerations for its core analysis" to deny institution based on petitioner's abusive filing practices). *Id.* at 1353. Thus, the Board had already found denial appropriate under Section 325(d) even before an *ex parte* reexamination was filed. In contrast here, there was no such finding by the Board.

Further, even after the *In re Vivint* Board denied three serial petitions under Section 325(d), petitioner "repackaged" its failed serial petition and filed it as an *ex parte* reexamination request, copying the petition almost word for word. *Id.* ("[Requestor's] *ex parte* reexamination request [is] another, fourth iteration of [its] abuse of process.") Petitioner's effective resubmission of its failed petition as a reexam request stood out to the Federal Circuit as an abusive filing. *Id.* Yet again, *In re Vivint* is distinguishable—here, the *ex parte* reexamination request includes new SNQs. These SNQs are based on the new primary prior art reference Ludtke, never before presented to the PTO. The reexamination request also addresses new claim construction issues first raised by the Board in its Institution Decision. This stands in stark contrast to the copy-and-paste request submitted in *In re Vivint.*

Patent Owner does not dispute these differences. Instead, Patent Owner attempts to liken Samsung's request to *In re Vivint* by alleging that Samsung's filing is a "serial" request merely because a prior IPR petition was filed. Pet. at 4. But Patent Owner cites no authority in support of this assertion. Indeed, if Patent Owner's argument were correct, then all *ex parte* reexam requests that follow an IPR petition would be denied as serial filings. Patent Owner cites no cases supporting such an extreme reading of Section 325(d).

IV. ROADMAPPING CONCERNS DO NOT APPLY TO SAMSUNG'S REQUEST

Next, Patent Owner argues that Samsung's request should be denied because Samsung improperly used the Board's Institution Decision as a "roadmap" to present the "same" arguments to the Office a second time.[2] Pet. at 4. To the contrary, Samsung's request presents substantial new questions of patentability not included in its IPR petition, as discussed above. Further, Samsung is not improperly using the Institution Decision as a "roadmap." Samsung's request properly addresses a new claim construction that was not available at the time Samsung's IPR petition was filed. Samsung had no prior opportunity to address this construction. Patent Owner has cited no authority supporting its argument that this is somehow improper. Patent Owner's argument is nothing more than a repackaging of its incorrect assertion that any *ex parte* reexamination request that follows an IPR petition must be denied.

Patent Owner also argues that the Board adopted Samsung's district court construction and, thus, Samsung should have included the art and arguments in its *ex parte* reexam request in its earlier IPR petition. But Samsung could not have foreseen the Board's construction of "third-party trusted authority," let alone the Board's application of that construction to the prior art, at least because Samsung's

[2] Notably, this assertion is internally inconsistent.

construction did not exist until two months after the IPR petition was filed. Patent Owner admits as much. *Compare* Pet. at 3 ("On August 26, 2021, Samsung filed a Petition for IPR") *with id.* at 4 ("Samsung was aware of its own proposed construction for the term "third-party trusted authority"...at least as of October of 2021."). Accordingly, there was no way for Samsung to foresee that the Board would adopt this construction, let alone predict a rejection based on it.

Further, Samsung could not have included its reexam request grounds based on Ludtke in its IPR petition at least because Samsung was not aware of this prior art until after the Board's Institution Decision. Patent Owner's suggestion that Samsung was aware of Ludtke simply because it is published prior art strains credibility—Section 325(d) does not assume that a requestor is aware of every published patent application in existence, and Patent Owner cites no authority supporting such an assertion.

V. DENIAL OF INSTITUTION BASED ON § 325(d) IS NOT WARRANTED

A. Patent Owner's Petition Relies On The Wrong Legal Standard

Patent Owner's petition seeks termination of these proceedings based on Section 325(d). But Patent Owner provides no analysis of Section 325(d) in its petition. Indeed, Patent Owner fails to mention the *Becton Dickinson* or *Advanced Bionics* factors at all, let alone provide rebuttal to Samsung's analysis.

Instead, Patent Owner analyzes the *General Plastic* factors. But, as Patent Owner admits, the *General Plastic* decision applies to 35 U.S.C. § 314(a) ***not*** Section 325(d).[3] Pet at n. 20. Thus, the *General Plastic* factors cannot be used to support Patent Owner's petition under Section 325(d). Patent Owner's failure to address the correct legal standard is fatal to its petition.

Further, even if *General Plastic* did apply, Patent Owner cites no precedent that *General Plastic* usurps *Becton Dickinson* or *Advanced Bionics*. Patent Owner instead makes the conclusory assertion that *General Plastic* should apply because it is directed towards "core considerations of impermissible roadmapping," citing *In re Vivint*. Pet. at n. 20. But Patent Owner's citation to *In re Vivint* misses the mark. *In re Vivint* did not hold that *General Plastic* should be used by the CRU to determine whether to deny institution under Section 325(d), and it certainly did not suggest that *Becton Dickinson* or *Advanced Bionics* could be ignored. Instead, *In re Vivint* merely found that the PTAB's ultimate conclusion in its institution decision was based on Section 325(d) in spite of the Board's discussion of Section 314(a). *See In re Vivint* at 1353 ("Though the Patent Office ostensibly applied §

---

[3] The Board's *NVIDIA* decision first set forth the seven factors made precedential by *General Plastic*. *See General Plastic* at 3. Notably, in *NVIDIA* the Board made clear that the seven *General Plastic* factors constitute a "separate" analysis from denials under Section 325(d). *NVIDIA Corp. v. Samsung Elec. Co.*, IPR2016-00134 (Paper 9) at 12 (PTAB May 4, 2016) (providing "***Separate*** Reasoning under 35 U.S.C. § 325(d)" for denial) (emphasis added).

314(a) to deny institution, it actually relied on § 325(d) considerations for its core analysis."). As discussed in Samsung's initial opposition, which remains unrebutted by Patent Owner, Section 325(d) considerations like those analyzed in *In re Vivint* support continuation of the instant reexamination proceedings.

In any case, even if *General Plastic* were controlling, the *General Plastic* factors ("GP Factors") weigh in favor of continuing reexamination.

1. GP Factor 1: Whether The Same Petitioner Previously Filed A Petition Directed To The Same Claims Of The Same Patent

Patent Owner does not analyze *General Plastic* Factor 1, which asks whether the same petitioner filed a repeat IPR petition at the PTAB addressing the same challenged claims. Instead, Patent Owner rewrites this factor to ask whether a requestor for *ex parte* reexamination had previously filed an IPR petition against the same challenged claims. This modification is not trivial—*General Plastic* does not compare the filing of two different types of submissions with different requirements before a different branch of the PTO. Patent Owner's self-serving modification transforms *General Plastic* into a much broader analysis of whether a party has ever challenged the same claims of a patent at any time before at the PTO. This is not the standard under *General Plastic* and, thus, Patent Owner's arguments regarding Factor 1 should be rejected.

Moreover, Patent Owner's argument appears to address a different set of patent claims from those at issue here. In particular, Patent Owner's petition makes arguments about "claims 12-17," and argues that the subject matter of "claim 15 presents…identical subject matter to the 11 claims that have already been…challenged." Pet. at 8. But the request challenges claims 1-18.

In any case, as discussed below, Samsung's request raises substantial new questions of patentability as to the challenged claims, which is the relevant inquiry for *ex parte* reexamination requests. Accordingly, any suggestion the instant request is the same or duplicative of Samsung's IPR petition is without merit. Thus, even Patent Owner's modified version of this factor weighs in favor of institution.

2. GP Factor 2: Whether At The Time Of Filing Of The First Petition The Petitioner Knew Of The Prior Art Asserted In The Second Petition Or Should Have Known Of It

Patent Owner does not argue that Samsung knew of the new prior art included in its request. Indeed, Samsung was not aware of Ludtke at the time it filed its IPR petition. Instead, Patent Owner suggests that because Ludtke was "publicly available" as a published application that Samsung should have known of it. But Patent owner does not cite a single case supporting the notion that mere public accessibility of a reference supports an inference that a requestor should have known about a prior art reference.

Indeed, if Patent Owner's interpretation were correct then this factor would always weigh in favor of denial, because all prior art submitted in a request must be "publicly available." Accordingly, this factor also weighs in favor of continuing reexamination.

3. GP Factor 3: Whether At The Time Of Filing Of The Request For Reexamination The Requestor Already Received The Patent Owner's Preliminary Response To The previous IPR Petition Or Received The Board's Decision On Whether To Institute Review

Here, again, Patent Owner rewrites the *General Plastic* factors to fit its incorrect narrative that *General Plastic* focuses on the interplay between IPRs and *ex parte* reexams. Factor 3 does not. Instead, it focuses on whether the same petitioner uses a Patent Owner's preliminary response and an Institution Decision as a roadmap to file a follow-on IPR petition before the statutory bar date. As discussed above, that is not the case here.

Samsung's request presents substantial new questions of patentability, relying on new art and addressing a new claim construction which was not available at the time the IPR petition was filed. Thus, there is no "roadmapping" or serial filings here. Accordingly, this factor weighs in favor of continuing reexamination.

4. GP Factor 4: The Length Of Time That Elapsed Between The Time The Petitioner Learned Of The Prior Art

Asserted In The Second Petition And The Filing Of The Second Petition

Patent Owner does not deny that Samsung filed its *ex parte* reexam request within three months of the Board's denial of institution. Patent Owner likewise does not contest that Samsung located the Ludtke reference after the Board's denial. Thus, there is no dispute that the *ex parte* reexamination request was filed mere weeks after Samsung learned of the prior art. Thus, this factor weighs in favor of institution.

5. GP Factor 5: Whether The Petitioner Provides Adequate Explanation For The Time Elapsed Between The Filings Of Multiple Petitions Directed To The Same Claims Of The Same Patent

As with the other factors, Patent Owner rewrites Factor 5 to require an explanation regarding the relative timing of an IPR petition and an *ex parte* reexam request. Factor 5 includes no such inquiry, instead asking about the relative timing of two IPR petitions directed towards the same claims.

There is no dispute that Samsung filed is request only weeks after discovery Ludtke. Thus, there is no delay. This factor weighs in favor of continuing reexamination even according to Patent Owner's modified standard.

6. GP Factor 6: The Finite Resources Of The Board

Patent Owner yet again rewrites the *General Plastic* factors, styling Factor 6 as an inquiry regarding the resources of the "*Office*." But *General Plastic*

concerns the resources of the "*Board*." Here, there are no wasted resources of the Board, because the request will not be considered by the Board. In any case, Patent Owner has failed to cite any case law suggesting a reexam request following an IPR represents wasted resources, especially where, as here, the reexam request substantial new questions of patentability based on prior art never presented to the Office addressing a new claim construction. Indeed, if Patent owner were correct, then this factor would always weigh against reexam when a previous IPR was filed.[4]

7. GP Factor 7: The Requirement For The PTAB To Issue A Final Determination No Later Than 1 Year After The Date On Which The Director Notices Institution Of Review

There is no dispute that *General Plastic* Factor 7, which addresses the PTAB's deadline to issue a final written decision, is not applicable here. This underscores the inapplicability of *General Plastic* to *ex parte* reexamination requests. Indeed, *General Plastic* was not issued with an eye towards addressing the interplay between *ex parte* reexamination requests and a prior IPR petition, let alone to serve as the basis for Section 325(d) analysis by the CRU; rather, *General Plastic* is aimed at preventing petitioners from making serial, abusive filings at the PTAB.

---

[4] Moreover, Patent Owner's arguments related to wasting resources ring hollow given Patent Owner's failure to follow the directives in the CRU's Decision, forcing Samsung and the CRU to address additional, unauthorized briefing.

VI. THE DIRECTOR SHOULD INVOKE HER OWN INITIATIVE UNDER 35 U.S.C. § 303(A)

Patent Owner admits that the "public interest" may weigh in favor of instituting an *ex parte* reexamination proceeding. Here, there is such an interest. As discussed above, Patent Owner has improperly filed two petitions in contravention to the CRU's express directives. Accordingly, the Director should deny Patent Owner's petition, at least to curb such abusive practices in the future. Terminating this proceeding based on an unauthorized petition would be against the public interest, as it would encourage patent owners to file multiple petitions irrespective of CRU authorization, wasting resources of parties and the CRU.

Further, Samsung's request presents strong grounds for invalidity. Indeed, the CRU has already granted reexam based on these substantial new questions of patentability. It is in the public interest that the CRU have an opportunity to reject invalid patents, such as this one, to ensure they do not serve as a roadblock to innovation or commerce.

VII. CONCLUSION

For the foregoing reasons, the CRU should reject Patent Owner's petition and proceed with *ex parte* reexamination.

DATED: October 4, 2022

Respectfully submitted,

By */s/ James M. Glass*

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan,LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.

Certificate of Service

The undersigned hereby certifies that, pursuant to the parties' stipulation permitting electronic service, on October 4, 2022, a copy of the foregoing was served via email to the addresses listed below:

Hecht Partners
David Hecht
Kinza Hecht
kinza@hard-ip.net
125 Park Avenue, 25th Floor
New York, NY 10017

Dated: October 4, 2022

By: */s/ Marissa Ducca*
Marissa Ducca
Reg. No. 59,807

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/015,053	06/08/2022	9298905	2090-0002-REX	7424

142179 7590 10/04/2022

Hard IP LLC (General)
10 Notch Hill Drive
Livingston, NJ 07039

EXAMINER	
RIMELL, SAMUEL G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/04/2022	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS

October 4, 2022

MARISSA R. DUCCA
QUINN EMANUEL URQUHART & SULLIVAN. LLP
1300 I STREET, NW SUITE 900
WASHINGTON, DC 20005

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 90015053
PATENT NO. : 9298905
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Decision on Petition for Extension of Time in Reexamination	**Application No.:** 90/015,053	**Applicant(s):** 9,298,905 B1	
	Examiner Samuel G. RIMELL	**Art Unit** 3992	

1. THIS IS A DECISION ON THE PETITION FILED 10/03/22.

2. THIS DECISION IS ISSUED PURSUANT TO:
   - A. ☒ 37 CFR 1.550(c) – The time for taking any action by a patent owner in a third party requested *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   - B. ☐ 37 CFR 1.550(c) – The time for taking action by a patent owner in a patent owner requested *ex parte* reexamination proceeding will only be extended for more than two months for sufficient cause and for a reasonable time specified.
   - C. ☐ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.

   The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS: Patent Owner requests that the time period for filing an optional Patent Owner's Statement, after the mailing of an "***Order Granting Request for Ex Parte Reexamination***" on 08/02/22, which is a two (2) month period pursuant to 37 CFR 1.530(b) (due 10/02/22), be extended by an additional one (1) month (due 11/02/22).
   - A. Petition fee per 37 CFR § 1.17(g)):
     - i. ☐ Petition includes authorization to debit a deposit account.
     - ii. ☒ Petition includes authorization to charge a credit card account.
     - iii. ☐ Other: _____.
   - B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
   - C. ☒ Petition was timely filed.
   - D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
   - A. ☒ Granted or ☐ Granted-in-part for ***one (1) additional month***. (See 37 CFR 1.550(c) and 37 CFR 1.956).
     - i. ☒ Other/comment: See below CONCLUSION.
   - B. ☐ Dismissed because:
     - i. ☐ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 3 above).
     - ii. ☐ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
     - iii. ☐ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
     - iv. ☐ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
     - v. ☐ The petition is moot.
     - vi. ☐ Other/comment: _____.

5. CONCLUSION: **The 10/03/22 "REQUEST FOR EXTENSION OF TIME UNDER 37 C.F.R. [§] 1.550(C)" is hereby granted for one (1) additional month for showing "sufficient cause" (i.e., 1). requested reasonable amount of time of one month, REQ., p. 1, 1st para.; 2). set forth factual accounting of reasonably diligent behavior including action(s) taken to provide Patent Owner's Statement, REQ., p. 1, "Patent Owner has been reasonably diligent in preparing statement" and p. 2, awaiting an expert's interpretation of the prior art which qualifies as an action taken related to Patent Owner's ability to respond; and 3). explained why, in spite of action(s) taken, additional time is needed, REQ., p. 2, "Patent Owner wishes to ensure consistency among the various proceedings by waiting until after it deposes Requestor's expert in the co-pending litigation to make its statement in this one"). See MPEP 2265 VI, 1st, 3rd, and 5th paras. Accordingly, the time period for Patent Owner to file an optional Patent Owner's Statement after the mailing of the 08/02/22 Order is extended for one (1) additional month from 10/02/22 to 11/02/22. Therefore, an optional Patent Owner's Statement after the mailing of the 08/02/22 Order is due by the end of the day on Wednesday, 11/02/22.**

Telephone inquiries with regard to this decision should be directed to Gay Ann Spahn at 571-272-7731 in the CRU.	/Gay Ann Spahn/, Supervisory Patent Reexamination Specialist, Central Reexamination Unit

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. PATENT NO.:	9,298,905	ART UNIT:	3992
CONTROL NUMBER:	90/015,053	CONF. NO.:	7424
FILING DATE:	October 23, 2014	EXAMINER:	RIMELL, SAMUEL G.

TITLE: **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

FILED ELECTRONICALLY

Mail Stop *Ex Parte* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF SERVICE ON THIRD-PARTY REQUESTOR

Dear Commissioner:

The undersigned, on behalf of the Patent Owner, hereby certifies that a copy of the following document is being served on the Third-Party Requestor by first class mail on October 3, 2022:

Request for Extension of Time under 37 CFR 1.550(c).

The name and addresses of the parties being served are as follows:

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005

Attorneys for Third-Party Requestor, Samsung Electronics America, Inc.

Respectfully submitted,

Hard IP LLC

Dated: October 3, 2022

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598
Email: kinza@hard-ip.net

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. Patent No.:	9,298,905	Examiner:	RIMELL, SAMUEL G.
Issued:	March 29, 2016	Art Unit:	3992
Application No.:	14/521,982	CONTROL NUMBER:	90/015,053
Filed:	October 23, 2014		
Title:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION		

REQUEST FOR EXTENSION OF TIME UNDER 37 C.F.R. 1.550(C)

Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Commissioner:

Patent Owner respectfully requests a one-month extension of time under 37 C.F.R. § 1.550(c) to file the statement by Patent Owner under 37 C.F.R. § 1.530.

Patent Owner has been reasonably diligent in preparing the statement. The above-identified patent is currently being asserted against the Requestor in a related proceeding ("co-pending litigation") before Hon. Alan Albright in the Western District of Texas.[1] The Request for *Ex Parte* Reexamination ("Request") was filed late in the co-pending litigation, which is presently scheduled for trial in January 2023, following the denial of three petitions for *inter partes* review on this and two other related patents filed by the Requestor. The Request was also filed *after* the one-year statutory period under 35 U.S.C. § 315(b) to file requests for *inter partes*

[1] *Proxense v. Samsung Electronics Co., Ltd. et al,* No. 6:21-CV-00210 (W.D. Tex.).

review. At the time the request was filed, fact discovery in the district court ("Court") case had begun.

During the last weeks of fact discovery, Requestor presented an alternative defense of non-infringement in the co-pending litigation. The relevant code to substantiate the defense was partially produced during the last week of fact discovery. The full code has yet to be produced. While the Court refused to stay the co-pending litigation in light of this proceeding, the Court extended discovery as to permit Requestor time to file new interrogatories and present additional evidence. Additionally, the Court permitted a second track for expert discovery.

Patent Owner has yet to depose Requestor's expert, who has presented opinions regarding prior art asserted in the Request and the general state of the art at the time of filing—all of which may bear on Patent Owner's approach in this *Ex Parte* Reexamination proceeding. The deposition will permit Patent Owner to better understand the asserted prior art (and the Requestor's interpretation thereof) as well as the validity of Requestor's views regarding the state of the art at the time of filing.

Patent Owner believes strongly in the duty of candor under 37 C.F.R. § 1.56. Patent Owner wishes to ensure consistency among the various proceedings by waiting until after it deposes Requestor's expert in the co-pending litigation to make its statement in this one. As such, Patent Owner respectfully request a one-month extension of time under 37 C.F.R. § 1.550(c) as to permit discovery to close in the co-pending litigation thereby allowing Patent Owner to file a Statement fully apprised of the asserted references, state of the art at the time of filing, and other relevant facts.

Deposit Account Authorization

Authorization is hereby given to charge Deposit Account No. 60-0366 for any charges or shortages in fees that may be due.

Respectfully submitted,

Hard IP LLC

Dated: October 3, 2022

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598

Electronic Patent Application Fee Transmittal					
Application Number:	90015053				
Filing Date:	08-Jun-2022				
Title of Invention:	Biometric personal data key (PDK) authentication				
First Named Inventor/Applicant Name:	9298905				
Filer:	Kinza Hecht				
Attorney Docket Number:	2090-0002-REX				
Filed as Large Entity					
Filing Fees for ex parte reexam					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PETITION FEE- 37 CFR 1.17(G) (GROUP II)	1463	1	220	220
Miscellaneous:				
		Total in USD ($)		**220**

Electronic Acknowledgement Receipt	
EFS ID:	46744736
Application Number:	90015053
International Application Number:	
Confirmation Number:	7424
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	9298905
Customer Number:	142179
Filer:	Kinza Hecht
Filer Authorized By:	
Attorney Docket Number:	2090-0002-REX
Receipt Date:	03-OCT-2022
Filing Date:	08-JUN-2022
Time Stamp:	21:06:04
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$220
RAM confirmation Number	E202203L06290578
Deposit Account	600366
Authorized User	Kinza Hecht
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	905_Certificate_of_Service_of_Petition.pdf	24755 cc83fb0cfa9ead02856f2606abfc285b1a6d25d3	no	2
Warnings:					
Information:					
2	Reexam Request for Extension of Time	EOT_905.pdf	129163 fa2589bae2eb6624644192a905a4156ea5621a6e	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	37945 fc0b8d66c28be114f0f05fad6551bdc9c673bbc3	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	191863		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Attorney Docket No.: 2090-0002
Control No.: 90/015,053 (Re-exam of U.S. Pat. No. 9,298,905)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. Patent No.:	9,298,905
Issued:	March 29, 2016
Application No.:	14/521,982
Filed:	October 23, 2014
Title:	BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

Examiner:	RIMELL, SAMUEL G.
Art Unit:	3992
CONTROL NUMBER:	90/015,053

PETITION TO THE DIRECTOR UNDER 1.181(a)(2)
TO EXERCISE HER DISCRETION UNDER 35 U.S.C. § 325(d)

Mail Stop Petitions
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Commissioner:

Proxense, the owner of U.S. Patent 9,298,905 ("905 Patent") respectfully petitions the Director to exercise her discretion under 35 U.S.C. § 325(d) to terminate all proceedings relating to the Request for *Ex Parte* Reexamination filed by Samsung Electronics America, Inc. ("Samsung") on June 8, 2022, as improper under 35 U.S.C. § 325(d) in view of Samsung's denied Petition for *Inter Partes* Review, filed August 26, 2021.

TABLE OF CONTENTS

I. Petition for the Director to Exercise her Discretion under 35 U.S.C. § 325(d) to Terminate proceedings relating to Samsung's Request for *Ex Parte* Reexamination 3

A. Background and Applicability of In re Vivint 3

B. Under Section 325(d), the Director Should Exercise Discretion to Terminate the Current Proceedings 5

C. An Analysis Under Section 325(d) Involves Application of the *General Plastic* Factors, And Demands Termination of These Proceedings 7

1. Factor 1 – Whether the Requestor Previously filed a Petition Directed to the Same Claims of the Same Patent 7

2. Factor 2 – Whether at the Time of Filing of the Petition the Requestor Knew of the Prior Art Asserted in the Request for Reexamination or Should Have Known of It 8

3. Factor 3 – Whether at the Time of Filing of the Request for Reexamination the Requestor Already Received the Patent Owner's Preliminary Response to the Previous IPR Petition or Received the Board's Decision on Whether to Institute Review 10

4. Factor 4 – The Length of Time that Elapsed between the Time the Requestor Learned of the Prior Art Asserted in the Request and the Filing of the Request for Reexamination 12

5. Factor 5 – Whether Requestor Provides Adequate Explanation for the Time Elapsed between the Filing of Multiple Challenges Directed to the Same Claims of the Same Patent 12

6. Factor 6 – The Finite Resources of the Office 14

7. Factor 7 – The Requirement under 35 U.S.C. § 316(a)(11) to Issue a Final Determination Not Later than 1 Year after the Date on Which the Director Notices Institution of Review 15

D. The Director Should Not Invoke Her Own Initiative Authority under 35 U.S.C. § 303(a) 15

II. Conclusion 16

I. PETITION FOR THE DIRECTOR TO EXERCISE HER DISCRETION UNDER 35 U.S.C. § 325(D) TO TERMINATE PROCEEDINGS RELATING TO SAMSUNG'S REQUEST FOR EX PARTE REEXAMINATION

Patent Owner submits this Petition seeking termination pursuant to 35 U.S.C. § 325(d) of proceedings related to Samsung's Request for *Ex Parte* Reexamination of the 905 Patent (the "Request") in view of Samsung's denied Petition for *Inter Partes* Review of the same patent.

A. Background and Similarity to In re Vivint

On August 26, 2021, Samsung filed a Petition for IPR ("IPR Petition") challenging claims 1-12 of the 905 Patent based on two combinations of prior art references.[1] Samsung filed its IPR Petition approximately six months after being served with Proxense's complaint for patent infringement.[2] Samsung's Petition for IPR was denied.[3] The PTAB's non-institution decision issued on February 28, 2022, days before the end of the 35 U.S.C. § 315(b) statutory period. Three months later, on June 8, 2022, Samsung made a second attempt to challenge the claims of the 905 Patent, this time in the form of a Request for *Ex Parte* Reexamination. Samsung's request uses information gleaned from the PTAB's decision as a roadmap to bolster challenges it advanced unsuccessfully.

In its serial Request, Samsung openly admitted that its arguments had been crafted to overcome the PTAB's reasoning in the denial of Samsung's IPR Petition. In particular, Samsung claimed to be using that time to "search[] for any references which meet the 'third-party trusted authority' limitation as construed by the PTAB".[4] Samsung has purposely omitted from its June

---

[1] *Samsung Electronics America, Inc. v. Proxense, LLC,* IPR2021-01447 (PTAB February 28, 2022) (Paper 1).
[2] *See Proxense, LLC v. Samsung Electronics Co. Ltd. et al.*, No. 6:21-cv-00210-ADA, ECF No. 1 (W.D. TX) (complaint served as of March 12, 2021).
[3] *See* Case IPR2021-01447, Paper 12 (DI).
[4] Def's Opp'd Mot. for Leave to Am. Invalidity Contentions, 5, *Proxense v. Samsung Electronics Co., LTD,* No. 6:21-cv-00210-ADA, ECF No. 64, (W.D. Tex. Waco Div.)

8, 2022 Request the fact that the PTAB adopted the construction that ***Samsung*** proposed to the District Court during *Markman* briefing in October of 2021.[5] Samsung's claim that it could not have foreseen that construction is false. Samsung was aware of its own proposed construction for the term "third-party trusted authority"—and thus the scope of prior art that would be relevant to any challenge Samsung might seek to bring—at least as of October of 2021. Furthermore, Samsung's claim that its proposed construction somehow contradicted Patent Owner's construction has no basis in fact nor has Samsung provided any citation. The Board denied Samsung's IPR Petition for at least the reason that the art Samsung selected did not disclose, alone or in combination, a "third-party trusted authority."[6] Samsung's latest attempt to challenge the 905 Patent uses information gleaned from the PTAB's decision as a roadmap to bolster the same argument it previously presented—that the prior art discloses a "third-party trusted authority." **This is the same behavior that led to termination of Alarm.com's *ex parte* reexamination of Vivint's patents in *In re Vivint*.**[7]

The facts underlying *In re Vivint* are substantially similar to those presented here.[8] Like in *Vivint*, here Samsung sought to invalidate a patent on two obviousness grounds in a Petition for IPR, was denied, and used that denial to roadmap a request for *ex parte* reexamination of the same patent. This is just like *In re Vivint,* where Alarm.com's "undesirable, incremental petitioning" which "used prior Board decisions as a roadmap to correct past deficiencies" were doomed to fail.[9]

---

[5] *See* Case IPR2021-01447, Paper 12 (DI), Slip Op. at 12.
[6] Case IPR2021-01447, Paper 12 (DI), Slip Op. at 25.
[7] *In re Vivint,* 14 F.4th 1342, 1353 (Fed. Cir. 2021).
[8] *See id.* and *Alarm.com Inc. v. Vivint, Inc.,* IPR2016-01091.
[9] *See Alarm.com Inc. v. Vivint, Inc.,* IPR2016-01091, Slip Op. 8 ("In the '1997 petition, filed September 28, 2015, Petitioner challenged claims 1 and 4–21 of the '513 patent as anticipated by Scadaware,10 claims 2 and 3 as obvious over Scadaware and Austin, 11 and claims 8–21 as

Despite the striking similarities to *In re Vivint*, on August 2, 2022 the Central Reexamination Unit ("CRU") granted Samsung's Request for *Ex Parte* Reexamination. In that decision, the CRU briefly addressed the impact of Section 325(d), acknowledging that the PTAB denied IPR on the grounds that neither combination involving Scott or Scott and Robinson disclosed or taught a "third-party trusted authority."[10] The CRU also specifically acknowledged Samsung's express admission that its Request for *Ex Parte* Reexamination "presents newly cited Ludtke ***to address the omission [i.e. third-party trusted authority] identified as the basis for the Board's refusal to institute.***"[11] The CRU did not address *In re Vivint*, however. On July 22, 2022, Patent Owner filed a petition pursuant to Rule 1.183 to suspend and/or waive Rules 1.530(a) and (c) and to allow Patent Owner to file, and the Office to consider, a petition pursuant to 37 C.F.R § 1.181 requesting that the Director exercise her discretion under Section 325(d) to terminate the current proceedings prior to a determination under 37 C.F.R. § 1.515.[12]

B. The Director Should Exercise Her Discretion Under Section 325(d) to Terminate the Current Proceedings

Section 325(d) applies to requests for *ex parte* reexamination.[13] When determining whether to initiate or order a proceeding such as an *ex parte* reexamination, Section 325(d) permits the Director to "take into account whether, and reject the petition or request because, the same or

---

obvious over Scadaware and Garton... In the '129 petition, filed November 2, 2015, Petitioner challenged claims 1–9, 13, 15, 16, and 19–21 as anticipated by Johnson;12 claims 10– 12, 14, 17, and 18 as obvious over Johnson and Joao; and claim 14 as obvious over Johnson, Joao, and BACnet."). Here, Samsung also presented two challenges but in a single petition for IPR, rather than dividing them into two petitions as was the case in *In Re Vivint*.

[10] Order Granting Request for *Ex Parte* Reexamination, mailed August 2, 2022, page 11.

[11] *Id.* at page 12.

[12] The CRU's decision did not acknowledge or otherwise address any arguments raised in Patent Owner's July 22, 2022 petition pursuant to Rule 1.183

[13] *In re Vivint,* 14 F.4th 1342, 1354 (Fed. Cir. 2021) ("Section 325(d) applies to both IPR petitions and requests for ex parte reexamination")

substantially the same prior arguments previously were presented to the Office." 35 U.S.C. § 325(d).[14] And where, as here, a Request presents "the same or substantially the same prior arguments" made previously, Section 325(d) authorizes the Director to terminate *ex parte* reexaminations even if a request presents a substantial new question of patentability.[15] This is consistent with the Office's previous decisions.[16]

Accordingly, a request for reexamination following a failed petition for IPR, as here, should be evaluated under § 325(d) even if a substantial new question of patentability is raised.[17] Furthermore, the request for reexamination must be evaluated in the same manner a subsequent petition for IPR would be evaluated.[18] At the heart of a § 325(d) analysis is a determination as to "whether [Requestor] uses information gleaned from [an] earlier decision to bolster challenges it advanced unsuccessfully."[19]

The law does not tolerate a petitioner like Samsung to use information learned from a previously unsuccessful IPR challenge as a roadmap for a subsequent reexamination request.

---

[14] In its Request, Samsung made the unsupported assertion that Section 325(d) did not apply because "Ludtke, is completely new and was not considered during the prosecution or presented in the previously filed IPR." Request for *Ex Parte* Reexamination, pg 31. Samsung's bald assertion does not, however, supersede Federal Circuit precedent that Section 325(d) authorizes termination even if a request presents a substantial new question of patentability. *See In re Vivint,* 14 F.4th at 1350.

[15] *See In re Vivint,* 14 F.4th at 1350.

[16] *General Plastics Co., Ltd. V. Canon Kabushiki Kaisha,* IPR2016-01357, FN 14 (PTAB Sept 6, 2017) (Paper 19) (precedential) ("Allowing similar, serial challenges to the same patent, by the same petitioner, risks harassment of patent owners and frustration of Congress's intention in enacting the Leahy-Smith America Invents Act.").

[17] *See In re Vivint,* 14 F.4th at 1350.

[18] *In re Vivint,* 14 F.4th at 1354 ("[T]he Patent Office, when applying § 325(d), cannot deny institution of IPR based on abusive filing practices then grant a nearly identical reexamination request that is even more abusive. We see no difference between the IPR and *ex parte* reexamination processes that would justify such conduct and nothing short of termination of the reexamination would be appropriate.").

[19] *In re Vivint,* 14 F.4th at 1353.

Here, Samsung is presenting the same or substantially similar argument (that the prior art discloses "third-party trusted authority") but with the benefit of the "information gleaned" (a new prior art reference) from a previous failure before the Office. Samsung's Request for *Ex Parte* Reexamination exemplifies (as both Samsung admitted and the CRU acknowledged) this impermissible practice of roadmapping via serial challenges to the same patent. Patent Owner therefore respectfully requests that the Director exercise her discretion under § 325(d) to terminate the present *Ex Parte* Reexamination.

C. An Analysis Under Section 325(d) Involves Application of the *General Plastic* Factors, And Demands Termination of These Proceedings

The CRU's determination that Samsung engaged in (impermissible) roadmapping to present a "new" version of the same arguments it previously made regarding "third-party trusted authority" is a sufficient basis to terminate the current proceedings. Furthermore, the CRU did not provide an analysis using the factors articulated in *General Plastics*. Such an analysis (presented below) also compels termination.[20]

1. Factor 1 – Whether the Requestor Previously filed a Petition Directed to the Same Claims of the Same Patent

On August 26, 2021, Samsung filed a petition for IPR challenging claims 1-12 of the 905 Patent based on two combinations of prior art references. Accordingly, the Request was Samsung's *second* effort to raise challenges against claims 1-12 of the 905 Patent. Notably,

[20] Although *General Plastics* addressed institution of IPR under 35 USC § 314, the factors articulated in that case were directed to the core considerations of impermissible roadmapping (Case IPR2016-01357, slip op. at 17 (PTAB Sept 6, 2017) (Paper 19) (precedential)) that the Federal Circuit found to be at the heart of the Section 325(d) analysis in both IPR petitions and requests for *ex parte* reexamination. *See In re Vivint,* 14 F.4th at 1353 ("Though the Patent Office ostensibly applied § 314(a) to deny institution, it actually relied on § 325(d) considerations for its core analysis. It reasoned that 'allowing similar, serial challenges to the same patent, by the same petitioner, risks harassment of patent owners and frustration of Congress's intent in enacting the AIA. That is the heart of a § 325(d) analysis." (internal citations omitted)).

Samsung has engaged in this same strategy with respect to two other members of the 905 Patent's family.

The Request for Reexamination also challenges claims 12-17. But these newly challenged claims are substantially similar to those previously cited. The only difference is newly challenged claim 15 presents a system utilizing the methods disclosed in previously challenged claims. Accordingly, the newly challenged patent claims contain identical subject matter to the 11 claims that have already been unsuccessfully challenged. This first factor, therefore, strongly favors terminating Samsung's requested reexamination.

2. Factor 2 – Whether at the Time of Filing of the Petition the Requestor Knew of the Prior Art Asserted in the Request for Reexamination or Should Have Known of It

Factor 2 of the analysis involves determining whether the requestor could have raised the new prior art references earlier.[21] The relevant consideration under this factor is not whether the references are new or raise a substantial new question of patentability. Rather, the relevant issue is whether the references "could have been found with reasonable diligence."[22] The prior art asserted by Samsung in its request includes one newly cited U.S. Patent and one newly cited published U.S. patent application. Publicly available U.S. patents/publications could have been found, and raised, in Samsung's IPR petition.

Samsung has not even attempted to explain why a reasonably diligent search could not have uncovered these so-called "new" references. The relevant inquiry is "whether they could have been found with reasonable diligence."[23] The newly asserted references are freely available

[21] Case IPR2016-01357, slip op. at 18 (Paper 19) (precedential) ("Considering other factors (i.e., factors 2, 4, and 5) allows us to assess and weigh whether a petitioner should have or could have raised the new challenges earlier.").
[22] Case IPR2016-01357, slip op. at 20 (Paper 19) (precedential).
[23] Case IPR2016-01357, slip op. at 20 (Paper 19) (precedential).

online and searchable via numerous online resources, including the USPTO's Full-Text and Image Databases. Samsung claims that its search for new prior art stemmed from the PTAB adopting a construction for "third-party trusted authority" that it could "not foresee[]," but as explained in the background section, the PTAB merely adopted a construction that Samsung itself had proposed in October 2021 during *Markman* briefing at the District Court. Samsung also claims that this construction contradicted Patent Owner's proposed construction, but provides no evidence of this because it is false. Samsung was, therefore, clearly on notice, at the latest, as of October 2021 of the potential scope and meaning of the term "third-party trusted authority" that the PTAB ultimately adopted – from Samsung. Samsung was also, therefore, on notice as of October 2021 that art like Ludtke could have and should have been cited in its IPR petition.

Moreover, what bearing the PTAB's claim construction had on whether the newly asserted references could have been located earlier is not explained in Samsung's Request. This alone heavily weighs against Samsung's Request.[24]

Samsung wholly ignores the inquiry of whether it could have previously uncovered the two "new" references previously. Instead, Samsung purports to escape the application of § 325(d) merely because "in all four SNQs presented in this reexam, the primary reference, Ludtke, is completely new and was not considered during the prosecution or presented in the previously filed IPR".[25] But this is not the law; the fact that the references were not previously raised, alone, does not immunize a Request from analysis under § 325(d).[26]

---

[24] *One World Technologies, Inc. v. The Chamberlain Group, Inc.* IPR2017-01546, Slip Op. 6 (PTAB Dec. 13, 2017) (Paper 10) (DI) (Finding the failure to explain "what bearing the Federal Circuit's claim construction (or those of the Board or District Court) had on whether the Kikuya reference reasonably could have located earlier" weighed against institution.).
[25] Request at 31.
[26] *In re Vivint.* 14 F.4th at 1350 (citing 35 U.S.C. § 325(d)) ("Even when an *ex parte* reexamination request presents a substantially new question of patentability, the Patent Office

Samsung admitted that it used Patent Owner's Preliminary Patent Owner Response and the Board's decision to deny institution to substitute alternative, public prior art references that could have been raised in its Petition for IPR.[27] Samsung is not permitted under § 325(d) to continually harass the Patent Owner by using the Patent Owner's Response and the Board's prior decision as a guide to alter serial challenges to the patent.

3. Factor 3 – Whether at the Time of Filing of the Request for Reexamination the Requestor Already Received the Patent Owner's Preliminary Response to the Previous IPR Petition or Received the Board's Decision on Whether to Institute Review

Samsung received both the Patent Owner's Preliminary Response and the Board's decision on its previously filed petition before filing this Request—and Samsung had several months to carefully consider them.[28] Samsung itself characterized the Request as "address[ing]" Patent Owner's arguments set forth in its Preliminary Response to Samsung's failed IPR petition.

> In the decision not to institute the IPRs, the Board found merit in the Patent Owner's argument … that the prior art did not disclose a 'third party trusted authority.' The present petition addresses Patent Owner's new argument with different prior art, and therefore presents substantial new questions of patentability.

Request, at 24-25.

'may reject the request because the same or substantially the same prior art or arguments previously were presented to' it.").

[27] Def's Opp'd Mot. for Leave to Am. Invalidity Contentions, 5, *Proxense v. Samsung Electronics Co., LTD,* No. 6:21-cv-00210-ADA, ECF No. 64 (W.D.Tex. Waco Div.) ("Samsung promptly began supplemental prior art searches in response to the IPR decisions, focusing on locating prior art that addressed the new and narrower construction adopted by PTAB. It timely served final infringement contentions on March 7, 2022. But it continued searching for any references which meet the "third-party trusted authority" limitation as construed by the PTAB".).

[28] Def's Opp'd Mot. for Leave to Am. Invalidity Contentions, 5, *Proxense v. Samsung Electronics Co., LTD,* No. 6:21-cv-00210-ADA, ECF No. 64 (W.D.Tex. Waco Div.) ("Once Samsung found this new prior art, Samsung conducted the necessary analysis, simultaneously drafting EPRs. As soon as the analysis was complete, Samsung promptly filed the EPRs on June 8, 2022 based on the supplemental prior art it located in response to the PTAB's claim constructions: US Patent No. 7,188,110 ("Ludtke") and US Patent Publication No. 2003/0196084 ("Okereke").").

Samsung's roadmapping goes even further. Later in its Request, Samsung noted the Board's construction of "third party trusted authority," summarized the Board's reasoning, and then states that Samsung "has applied this construction, in light of the Board's observations and analysis, to the prior art below."[29] Accordingly, at least *twice* in the Request Samsung plainly admits to using what it learned from its failed petition for IPR, including Patent Owner's arguments and the PTAB's previous decision, as a roadmap in preparing the current Request. This admitted impropriety goes to the very heart of the analysis under § 325(d). Allowing unlimited follow-on challenges would give "petitioners the opportunity to strategically stage their prior art and arguments in multiple [challenges], using our decisions as a roadmap, until a ground is found that result in the grant of review."[30]. Such a practice "risks harassment of patent owners and frustration of Congress's intent in enacting the AIA."[31].

Recognizing the impropriety of the Request, Samsung asserts "there are ***no*** SNQs that are 'word-for-word' copies of the IPR grounds, and indeed, the primary reference that forms that vast basis for the rejections is entirely different and thus do not, and could not, use the prior IPR petition denial as a 'roadmap.'"[32] Besides the inherent internal contradiction with the statements noted above, the distinction Samsung is attempting to draw has no legal merit or logical basis. Using the PTAB's previous decision as a roadmap does not require copying the denied petition word-for-word.[33] That is not the inquiry and "word-for-word" copying would never occur. After all, if the Board denied a petition, there is no advantage in copying it word-for-word. A serial petition

[29] Request. at 35-36.
[30] Case IPR2016-01357, slip op. at 17 (Paper 19) (precedential).
[31] *In re Vivint*, 14 F.4th at 1353.
[32] Request, at 32.
[33] *In re Vivint,* 14 F.4th at 1353 ("And for the portions it did not copy, Alarm.com 'used the Board decision as a roadmap to correct past deficiencies.'").

is one that makes changes gleaned from the denial to correct the past deficiencies. Samsung's argument that it did not "roadmap" because it did not copy previous arguments verbatim must fail.

4. Factor 4 – The Length of Time that Elapsed between the Time the Requestor Learned of the Prior Art Asserted in the Request and the Filing of the Request for Reexamination

Samsung does not indicate in the Request when it learned of the newly asserted U.S. patent and the newly asserted published U.S. patent application. The Director should certainly consider the fact that Samsung did not initially raise the prior art in its petition for IPR, filed on August 26, 2021, over 9 months prior to the Request. Nor did Samsung file a second IPR petition when it proposed its construction of "third-party trusted authority" in October of 2021. Rather than filing a second IPR within the Section 315(b) statutory period, Samsung instead filed the Request months after that deadline expired. As mentioned above, the new art cited in the current Request was, at all relevant times, readily available and findable through commonly available search methods—likely the ones Samsung employed.

Thus, and in particular because Samsung failed to identify when it learned of the allegedly new art, the, the fourth factor favors terminating Samsung's requested reexamination.

5. Factor 5 – Whether Requestor Provides Adequate Explanation for the Time Elapsed between the Filing of Multiple Challenges Directed to the Same Claims of the Same Patent

Samsung's Petition for IPR was filed August 26, 2021. The current Request for Reexamination was filed over nine months later, on June 8, 2022. This length of time strongly favors terminating Samsung's requested reexamination.

Samsung has not adequately explained why it waited over nine months to file this Request. Samsung's only purported excuse is that it "did not foresee, as it contradicted Patent Owner's claim construction arguments in litigation," the Board's finding the prior art asserted in Samsung's

previous Petition for IPR did not disclose "a third-party trusted authority."[34] To the extent this is meant to justify the timing of the Request, it is both disingenuous and not pertinent. Any consideration of Samsung's surprise must be based on whether, from an objective perspective in the context of the applicable law and facts, Samsung's alleged surprise is reasonable.[35] As noted above, Samsung's alleged surprise at the Board's adoption of the very construction it proposed is unreasonable.

Notably, after filing its Petition for IPR, Samsung filed, in the Western District of Texas the Declaration of Dr. Nielson, which stated: "the common use of the term 'third party' in the industry, which refers typically to an entity not directly involved in the transaction. This industry definition of 'trusted third party' focuses on the 'third party' as an entity with a responsibility separate from executing the transaction itself".[36] Samsung further argued before the District Court that the specification and prosecution history of the 905 Patent conforms with Dr. Nielson purported common use of the term in the industry. Notably, Patent Owner did not challenge Samsung's argument and the parties agreed on a construction before the conclusion of *Markman*. Yet, none of the grounds of invalidity Samsung asserted in the Petition for IPR included an entity or party separate from the principal parties of the transaction. Samsung, consequently, asserted grounds for invalidity inconsistent with the evidence and arguments subsequently presented to the District Court.

---

[34] Request, page 24.
[35] Case IPR2016-01357, slip op. at 21 (Paper 19) ("Petitioner's assertion that is was 'surprised' by our claim construction is unpersuasive, because it is not the pertinent issue. Rather, any such inquiry is directed to whether, from an objective perspective in the context of the applicable law and facts, Petitioner's alleged surprise is reasonable.").
[36] *See Proxense, LLC v. Samsung Electronics Co. Ltd. et al.*, No. 6:21-cv-00210-ADA, ECF No. 33-2 at ¶73 (W.D. TX) (Declaration of Dr. Nielson).

Under 37 C.F.R. § 42.51(b), "a party must serve relevant information that is inconsistent with a position advanced by the party during the proceeding concurrent with the filing of the documents or things that contains the inconsistency." Yet, Samsung did not provide the Declaration of Dr. Neilson, nor its Opening Claim Construction Brief, to the PTAB. As a result, Patent Owner submitted the Declaration of Dr. Neilson, Samsung's Opening Claim Construction Brief, and Proxense's Responsive Claim Construction Brief with its Preliminary Patent Owner's Response.

It was unreasonable for Samsung to assume that Patent Owner would not rely on Samsung's proposed constructions in its Preliminary Response. Proxense noted the points of agreement regarding the meaning of "third party trusted authority" as well as the points of disagreement. The PTAB noted the differences. Based on the points of agreement, the PTAB determined the prior art asserted by Samsung did not include a "third party trusted authority" providing an "access message." This should not—and could not—have come as a "surprise" to Samsung.

Samsung's sole excuse for delay, and therefore its purported surprise, cannot justify the time that elapsed between the Petition for IPR and its Request for Reexamination.

6. Factor 6 – The Finite Resources of the Office

Samsung had already tasked the PTAB with evaluating a petition for IPR of the 905 Patent and two of its family members. Having that petition denied, Samsung now seeks to task the CRU with the same tasks. Tasking the CRU with examining a patent already presented to the Board is an inefficient and wasteful use of the CRU's limited time. As such, this factor, which favors a one-bite-at-the-apple approach for petitioners and requesters alike, militates against the continued reexamination of the 905 Patent as requested by Samsung.

7. Factor 7 – The Requirement under 35 U.S.C. § 316(a)(11) to Issue a Final Determination Not Later than 1 Year after the Date on Which the Director Notices Institution of Review

As previously noted, Samsung's Petition for IPR of the 905 Patent was denied. The Director, therefore, has not noticed institution of review. As such, this factor is not applicable to the current Request.

D. The Director Should Not Invoke Her Own Initiative Authority under 35 U.S.C. § 303(a)

The Director's own initiative authority to order reexamination of a patent is separate from her discretion under § 325(d).[37] There can be a public interest in reexamination that goes beyond the proprietary of behavior of a particular challenger.[38] However, Samsung's Request fails to advance or argue any such public interest. Rather, Samsung asserts it was surprised by the PTAB's decision to deny institution of *inter partes* review and wants another bite at the 905 patent apple. Samsung has not shown how this benefits anyone's interests other than its own.

[37] *In re Vivint,* 14 F.4th at 1354 ("Notably, too, the second sentence of § 325(d), the basis of the discretion at issue in this case, does not apply to such 'own initiative' authority; it applies only to a 'petition or request,' which the Director may 'reject' because of serial filing of a challenger. 35 U.S.C. § 325(d).").
[38] *Id.*

II. CONCLUSION

In view of the foregoing, the Director should exercise her discretion under § 325(d) and terminate all proceedings relating to Samsung's request for *ex parte* reexamination on the grounds the reexamination is an undesirable, incremental challenge to the 905 Patent.

Respectfully submitted,

Hard IP LLC

Dated: September 20, 2022

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598
Email: kinza@hard-ip.net

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. PATENT NO.:	9,298,905	ART UNIT:	3992
CONTROL NUMBER:	90/015,053	CONF. NO.:	7424
FILING DATE:	October 23, 2014	EXAMINER:	RIMELL, SAMUEL G.

TITLE: **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

FILED ELECTRONICALLY

Mail Stop *Ex Parte* Reexam
ATTN: Central Reexamination Unit
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF SERVICE ON THIRD-PARTY REQUESTOR

Dear Commissioner:

The undersigned, on behalf of the Patent Owner, hereby certifies that a copy of the following document is being served on the Third-Party Requestor by first class mail on September 20, 2022:

1. Petition to the Director under 1.181(a)(2) to Exercise Her Discretion under U.S.C. § 325(d)
2. Exhibits 1001-1009

The name and addresses of the parties being served are as follows:

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005

Attorneys for Third-Party Requestor, Samsung Electronics America, Inc.

Respectfully submitted,

Hard IP LLC

Dated: September 20, 2022

/Kinza Hecht/
Kinza Hecht
Patent Agent
Reg. No. 62,325
Phone: (212) 321-0598
Email: kinza@hard-ip.net

Electronic Patent Application Fee Transmittal

Application Number:	90015053
Filing Date:	08-Jun-2022
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	9298905
Filer:	Kinza Hecht
Attorney Docket Number:	2090-0002-REX

Filed as Large Entity

Filing Fees for ex parte reexam

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PETITION IN REEXAM PROCEEDING	1824	1	2040	2040
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2040**

Electronic Acknowledgement Receipt	
EFS ID:	46644361
Application Number:	90015053
International Application Number:	
Confirmation Number:	7424
Title of Invention:	Biometric personal data key (PDK) authentication
First Named Inventor/Applicant Name:	9298905
Customer Number:	142179
Filer:	Kinza Hecht/Eddie Rowell
Filer Authorized By:	Kinza Hecht
Attorney Docket Number:	2090-0002-REX
Receipt Date:	20-SEP-2022
Filing Date:	08-JUN-2022
Time Stamp:	13:50:48
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2040
RAM confirmation Number	E20229JD51161800
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Other reference-Patent/Application/ Search Documents	1001-Paper-1-905-Petition.pdf	8441131 2c8d41d3f46289235c93292aa17ba692f08a75e4	no	57
Warnings:					
Information:					
2	Other reference-Patent/Application/ Search Documents	1002-03-05-2021-Complaint.pdf	772284 241af684bbf7d1cca0de9b51ecda8c51e3f68372	no	47
Warnings:					
Information:					
3	Other reference-Patent/Application/ Search Documents	1004-064-2022-08-05-Motion-to-Amend-Invalidity-Contentions.pdf	251546 6cc2f3810eb089fb6f6857e6d2a5569908cf5bf7	no	21
Warnings:					
Information:					
4	Other reference-Patent/Application/ Search Documents	1006-3-905-Request.pdf	938110 a055880ac07c71b71c54e6a87843131d142f13e9	no	92
Warnings:					
Information:					
5	Other reference-Patent/Application/ Search Documents	1007-PAPER-19.pdf	12932798 e2bde66d7c866b70185f8940c08fe2daf4395409	no	23
Warnings:					
Information:					
6	Other reference-Patent/Application/ Search Documents	1008-PAPER-10.pdf	5145685 192291c44450cb72ac4ff4d33dc92732ebdbc169	no	10
Warnings:					
Information:					

7	Other reference-Patent/Application/ Search Documents	1009-033-02-Exhibit-A.pdf	17659092 045d84c2caf1eff08a6c35d0729de55d38ee46e0	no	25
Warnings:					
Information:					
8	Other reference-Patent/Application/ Search Documents	1003-Paper-12-Decision-Denying-IPR.pdf	15313407 d3ff099ffbe1d85faab42f575193de2a9a6cc661	no	31
Warnings:					
Information:					
9	Other reference-Patent/Application/ Search Documents	1005-905-Reexam-Order.pdf	995022 07e3d5f5b15bfcf955f3e31dd9814e208846f9ca	no	16
Warnings:					
Information:					
10	Petition for review by the Office of Petitions	2022-09-20-905-EPR_Petition.pdf	194992 5f6bf30c3eba7331a460ada91501ac807ddf5e86	no	16
Warnings:					
Information:					
11	Reexam Certificate of Service	1-905_Certificate_of_Service_of_Petition.pdf	85044 924063dcbbb701fa17b6c1663788a2a9517495a5	no	2
Warnings:					
Information:					
12	Fee Worksheet (SB06)	fee-info.pdf	37898 e18022940f54c82d649e9c45e904dfee1c7c5284	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	62767009		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC,
Petitioner

v.

PROXENSE, LLC
Patent Owner

IPR2021-01447
Patent No. 9,298,905

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,298,905 UNDER 35 U.S.C § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

I. INTRODUCTION 1

II. MANDATORY NOTICES 2

A. Grounds for Standing (37 C.F.R. § 42.104(a)) 2

B. Real Party in Interest 3

C. Related Matters 3

D. Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4)) 3

E. Payment of Fees (37 C.F.R. § 42.15(a)) 4

III. LEVEL OF SKILL IN THE ART 4

III. IDENTIFICATION OF CHALLENGE AND RELIEF REQUESTED 5

IV. OVERVIEW OF THE '905 PATENT 6

A. Prosecution History 6

V. CLAIM CONSTRUCTION 7

VI. CITED ART 8

A. Scott (WO1999056429) 8

B. Lapsley (US2001/0000535) 8

C. Robinson (US2003/0177102) 9

D. Berardi (US7239226) 10

E. Shreve (US2002/0109580) 10

F. Kinoshita (US2003/0055792) 11

G. Enablement 11

VII. DISCRETIONARY FACTORS 12

A. 35 U.S.C. § 325(d) Does Not Favor Denial 12

B. 35 U.S.C. § 314(a) Does Not Favor Denial 13

VII. DETAILED EXPLANATION OF GROUNDS FOR INVALIDITY 19

A. Ground 1: Claims 1, 3-10, and 12 are rendered obvious by Scott and Lapsley. 19

B. Ground 2: Claims 2 and 11 are rendered obvious by Scott, Lapsley, and Robinson. 34

C. Ground 3: Claim 1 and 3-7 are rendered obvious by Berardi, Shreve, and Kinoshita. 36

VIII. SECONDARY CONSIDERATIONS 47

IX. CONCLUSION 47

EXHIBIT LIST

No.	Exhibit
1001	U.S. Patent No. 9,298,905
1002	File History for U.S. Patent No. 9,298,905
1003	Declaration of Andrew Wolfe, Ph.D.
1004	Curriculum vitae of Andrew Wolfe, Ph.D.
1005	International App. No. WO 1999056429 to Scott et al.
1006	Intentionally Left Blank
1007	U.S. Patent Pub. No. 2001/0000535 A1 to Lapsley et al.
1008	U.S. Patent Pub. No. 2003/0177102 A1 to Robinson
1009	Intentionally Left Blank
1010	U.S. Patent No. 7,239,226 B2 to Berardi et al.
1011	Intentionally Left Blank
1012	U.S. Patent Pub. No. 2002/0109580 A1 to Shreve et al.
1013	U.S. Patent Pub. No. 2003/0055792 A1 to Kinoshita et al.
1014	"Applied Cryptography—Protocols, Algorithms, and Source Code in C" (1996) by Schneier
1015	Declaration of Sylvia Hall-Ellis, Ph.D.
1016	Intentionally Left Blank

LIST OF CHALLENGED CLAIMS

Claim	U.S. Patent No. 9,298,905
1pre	A method comprising:
1A	persistently storing biometric data of a legitimate user and an ID code on an integrated device;
1B	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
1C	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
1D	responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
1E	responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.
2	The method of claim 1, further comprising: registering an age verification for the user in association with the ID code.
3	The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.
4	The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
5	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
6	The method of claim 1, wherein completing the financial transaction includes accessing an application.

7	he method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
8pre	The method of claim 1, further comprising:
8A	responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and
8B	wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
9pre	An integrated device comprising:
9A	a persistent storage media that persistently stores biometric data of a user and an ID code;
9B	a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, a validation module . . .that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
9C	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction.
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.
11	The integrated device of claim 7, wherein an age verification is registered in association with the ID code.
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

GROUNDS OF CHALLENGE (37 C.F.R. § 42.204(b)(2))

No.	Ground for Challenge
1	Scott and Lapsley render obvious Claims 1, 3-10, and 12
2	Scott, Lapsley, and Robinson render obvious Claims 2 and 11
3	Berardi, Shreve, and Kinoshita render obvious Claims 1, 3-7, 9-10, and 12

I. INTRODUCTION

The claims of the '905 patent relate to preventing unauthorized use of a wireless device by verifying both biometric data and the device itself. The '905 patent describes biometric authentication of a user of a wireless device using a generic "computerized authentication" system that provides secure access to resources such as ATMs and locked areas. Ex. 1001 ('905 Patent) at 1:21-24, 1:56-58. The wireless device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:64-2:5. Next, the wireless device transmits an ID code to a third-party to indicate that the user's identity has been verified. *Id.* If the third-party determines that the code is authentic, access is granted to the user to a secure resource. *Id.* at 2:6-14. The '905 patent purports to solve the problem of users having to "memorize or otherwise keep track of the[ir] credentials," *id.* at 1:33-35, 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." *Id.* at 1:46-48.

But this type of biometric authentication system was known years before the '905 patent was filed. For example, in 1999—five years before the '905 patent's earliest filing date—the Scott reference disclosed a wireless personal identification device that verified biometric data of user via a biometric scan and authenticated the user for access to protected resources such as a hotel room or an electronic

transaction. Likewise, the Berardi reference also expressly discloses verifying biometric data and authenticating a user by means of a third-party trusted agent to provide access to a secure resource. In fact, numerous prior art patents teach the same concept. For example, the Shreve and Kinoshita reference uses similar portable devices in secure authentication processes.

Thus, the challenged claims merely recite the well-known concept of verifying biometric data and authenticating a user's device using a third-party trusted agent—well-worn concepts known in the art years before the '905 patent was filed. Accordingly, the challenged claims should be held unpatentable.

II. MANDATORY NOTICES

Pursuant 37 C.F.R. § 42.8(a)(1), the following mandatory notices are provided as part of this Petition.

A. Grounds for Standing (37 C.F.R. § 42.104(a))

Samsung Electronics America, Inc. ("Samsung" or "Petitioner") respectfully requests *inter partes* review ("IPR") of Claims 1-12 ("Challenged Claims") of U.S. Patent No. 9,298,905 to Giobbi ("the '905 Patent") (Ex. 1001), which is indicated as assigned to Proxense LLC. ("Patent Owner" or "Proxense").

Petitioner certifies that the '905 Patent is available for *inter partes* review and Petitioner is not barred or estopped from requesting review of the Challenged Claims on the grounds identified in this Petition.

B. Real Party in Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies Samsung Electronics, Co., Ltd. and Samsung Electronics America, Inc. are the real parties-in-interest.

C. Related Matters

The '905 patent has been asserted against Petitioner in: *Proxense, LLC v. Samsung Electronics, Co., Ltd. et al.*, No. 6.21-CV-00210 (W.D. Tex. March 5, 2021).

Moreover, Patent Owner also has asserted U.S. Patent Nos. 9,049,188; 9,235,700; 8,352,730; and 10,698,989 in the above litigation, and Petitioner also is concurrently filing a petition challenging that patent.

D. Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4))

Petitioner provides the following counsel and service information. Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition. Petitioner agrees to accept electronic service at the email addresses listed below.[1]

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46729) jimglass@quinnemanuel.com Postal and Hand Delivery Address:	Marissa Ducca (Reg. No. 59,807) marissaduca@quinnemanuel.com Richard Lowry (Reg. No. 70,306)

[1] Petitioner consents to electronic service to ge-samsung-proxense@quinnemanuel.com and the email addresses listed in the table below.

QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Ave, 22nd Floor New York, New York 10010 Tel: (212) 849-7000 Fax: (212) 849-7100	richardlowry@quinnemanuel.com Postal and Hand Delivery Address: QUINN EMANUEL URQUHART & SULLIVAN, LLP 1300 I St. NW Washington, DC 20005 Tel: (202) 538-8000 Fax: (202) 538-8100 Sean Gloth (Reg. No. 75,316) seangloth@quinnemanuel.com Postal and Hand Delivery Address: QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Ave, 22nd Floor New York, New York 10010 Tel: (212) 849-7000 Fax: (212) 849-7100

E. Payment of Fees (37 C.F.R. § 42.15(a))

The undersigned authorizes the Office to charge the fee required for this Petition for *Inter Partes* Review to Deposit Account No. 50-5708. Any additional fees that might be due are also authorized.

III. LEVEL OF SKILL IN THE ART

Petitioner proposes that a Person of Ordinary Skill in the Art would have had a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). Petitioner further proposes that more education could compensate for less experience and vice versa.

III. IDENTIFICATION OF CHALLENGE AND RELIEF REQUESTED

Petitioner challenges claims 1-12 of the '905 Patent and requests that these claims be found unpatentable in view of the following references:

1. PCT Application No. WO 99/56429 to Scott et al., filed April 26, 1999 and published November 4, 1999 (Ex. 1005, hereinafter "Scott");
2. US Patent Application Publication No. US 2001/0000535 to Lapsley et al., filed December 6, 2000 and published April 26, 2001 (Ex. 1007, hereinafter "Lapsley")
3. US Patent Application Publication No. US 2003/0177102 to Robinson, filed February 19, 2003 and published September 18, 2003 (Ex. 1008, hereinafter "Robinson")
4. US Patent No. US 7,239,226 to Berardi et al., filed July 9, 2002 and published July 3, 2007. (Ex. 1010, hereinafter "Berardi")
5. US Patent Application No. US 2002/0109580 to Shreve et al., filed February 15, 2001 and published August 15, 2002. (Ex. 1012, hereinafter "Shreve")
6. US Patent Application Publication No. US 2003/0055792 to Kinoshita et al., filed July 19, 2002 and Published March 20, 2003. (Ex. 1013, hereinafter "Kinoshita")

Pursuant to §§42.22(a)(1) and 42.22(b)(1)-(2), Petitioner requests cancellation of claims 1-12 of the '905 Patent on the following grounds:

Ground 1: 1, 3-10, and 12 are rendered obvious by Scott and Lapsley.

Ground 2: Claims 2 and 11 are rendered obvious by Scott, Lapsley, and Robinson.

Ground 3: Claim 1, 3-7, 9-10, and 12 are rendered obvious by Berardi, Shreve, and Kinoshita.

IV. OVERVIEW OF THE '905 PATENT

As explained herein, the '905 patent relates to integrated wireless devices in a generic "computerized authentication" system that are used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 ('905 Patent) at 1:21-24, 1:56-58. The device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:64-2:5. After validation, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* The device transmits the code to a third-party trusted key authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 2:6-14. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* The '905 patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:33-35. The patents also purport to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:46-48.

A. Prosecution History

The '905 Patent was filed on October 23, 2014 and claimed the benefit of application no 60/637,538 filed on December, 2004. Ex. 1002 at 482.

On June 12, 2015, after lengthy exchange regarding various formalities, the U.S. Patent & Trademark Office (hereinafter "Patent Office") issued the first non-final Office Action rejecting claims 2-18 under 35 U.S.C 103 in light of Hsu et al. (US 6,041,410) in view of Saito et all (US 20040129787) as well as non-statutory double patenting in light of US Patent No. 8,886,954. Ex. 1002 at 94--86.

After amendment and an examiner-initiated interview to suggest terminal disclaimers the Patent Office issued a Notice of Allowance on December 16, 2015. Ex. 1002 at 37-47 and 76-80.

V. CLAIM CONSTRUCTION[2]

Petitioner submits that express interpretations of the challenged claims are not required to resolve this petition. Because no constructions are necessary to resolve this petition, Petitioner proposes that the claim terms should be given their plain and ordinary meaning. Petitioner reserves its right to respond to any claim constructions raised by the Patent Owner or the Board in the future.

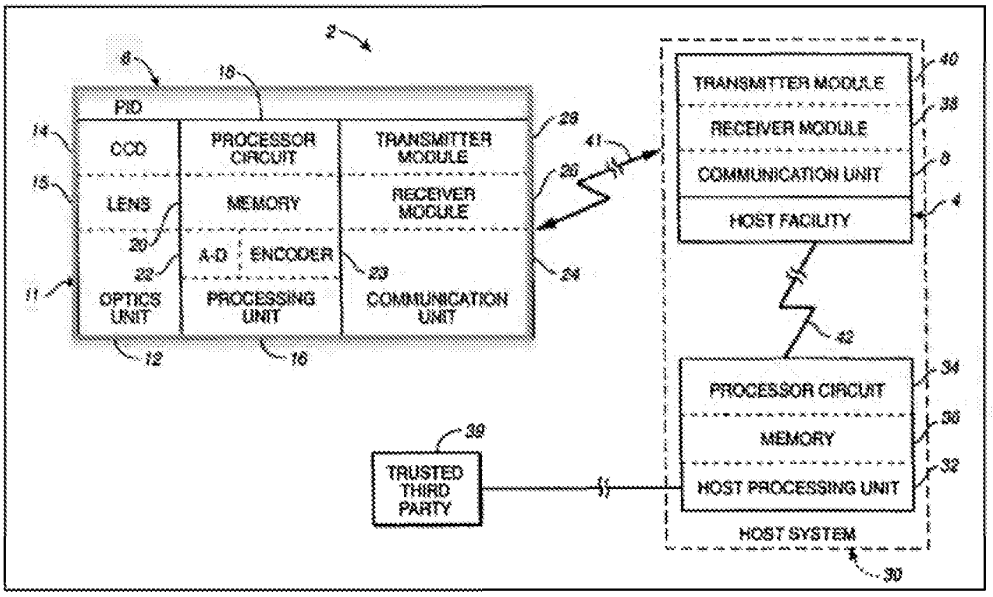
---

[2] Petitioners reserve the right to pursue different claim constructions, including that certain claim terms are indefinite, during this and related proceedings as well as in any district court litigation concerning the '905 Patent. *See Samsung Elecs. Am., Inc. v. Prisua Eng'g Corp.*, 948 F.3d 1342, 1350 (Fed. Cir. 2020) ("[T]he Board may not cancel claims for indefiniteness in an IPR proceeding.").

VI. CITED ART

A. Scott (WO1999056429)

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1005 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1E] *infra*.



Ex. 1005 at Fig. 1.[3]

B. Lapsley (US2001/0000535)

Lapsley discloses a third-party authentication system to validate a transaction initiated at a biometric device (*i.e.*, Party Identification Apparatus

[3] Annotations are added to figures unless indicated otherwise.

(PIA)). Ex. 1007 at Abstract, ¶54. The PIA includes a biometric sensor that receives a user's biometric input accompanying an electronic payment. *Id.* at ¶167. The PIA transmits the biometric data and a PIA hardware identification code to a trusted third-party Data Processing Center (DPC). *Id.* at ¶168. The DPC includes a list of hardware identification codes for PIAs, wherein each respective code "makes the PIA uniquely identifiable to the DPC in all transmissions from that device." *Id.* at ¶¶85, 161. Using this list, the DPC identifies the PIA by its PIA hardware identification code. *Id.* at ¶¶85, 103, 104, 158, 166. Lapsley also discloses that communication security is achieved using an encryption scheme that uses public/private keys and admits doing so is "well known in the industry." *Id.* at ¶82.

C. Robinson (US2003/0177102)

Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1008 at ¶¶27-28, 32, 66-67 Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses

that age-verifying information is associated with at least one ID number (SID) identifying the user.

D. Berardi (US7239226)

Berardi discloses a method for verifying a user during authentication of an integrated device (*e.g.*, portable electronic Fob 102) that engages with RFID reader 104 to, for example, facilitate a point-of-sale transaction. Ex. 1010 at Abstract, 3:45-4:3, 12:36-48, Fig. 2. Berardi further discloses the conventional encryption techniques may be used, such as those described in the text "Applied Cryptography: Protocols, Algorithms, and Source Code in C," written by Bruce Schneier (second edition, 1996)[4], which Berardi incorporates by reference. *Id.* at 7:19-27. The fob 102 is thus useful for completing a contactless transaction and would ordinarily be carried by a user for verification. Ex. 1010 at 1:15-18, 1:32-36.

E. Shreve (US2002/0109580)

Shreve discloses a transceiver/fob device 12, which is "a remote keyless entry-based transceiver device," capable of two-way wireless communications with domain system 14 for secure access authorization based on biometrics. Ex. 1012 at Fig. 2a, ¶¶33, 35. Shreve discloses a service provider 24 with a secured database

[4] Schneier was publicly available before the filing of the patent at issue. Ex. 1015.

31 that provides authentication of a transaction initiated by a fob device 12. *Id.* at ¶39. For authentication, the database 31 contains cross-references between "the key fob ID and other user specific information (e.g., accounts, access privileges, biometrics, etc) that can be used by the authentication algorithm **23** to further facilitate the authentication process." *Id.* at ¶39, claim 47.

F. Kinoshita (US2003/0055792)

Kinoshita discloses a portable device 14 that authenticates a user before transmitting a user ID to a POS terminal 11, which forwards the user ID to a third-party payment gateway 15 to authorize a payment transaction. Ex. 1013 at ¶¶168-69, Fig. 1. Specifically, the payment gateway 15 confirms the authenticity of the portable device 14 by comparing the device ID of the portable device 14 to stored device ID in a user table 154a. *Id.* at ¶171. After the payment gateway 15 receives a user ID and a request for transaction, the payment gateway 15 sends an e-mail message that includes commands for direction of payment to be executed by the portable device 14. ¶¶168-69. Upon receiving the e-mail message, the portable device 14 "executes an application for payment according to the commands included in the e-mail." *Id.* at ¶¶168-69, 179-83.

G. Enablement

The above described reference both individually and in the combinations explained below enable the systems and methods they are cited for. Ex. 1003.

None of the above-mentioned references describe an aspirational or otherwise unachievable system or method. *Id.* To the extent Patent Owner argues that any of the above described references are not self-enabled or otherwise do not satisfy *Raytheon Techs. Corp. v. Gen. Elec. Co.*, 993 F.3d 1374 (Fed. Cir. 2021), a POSITA would have understood how to combine the references to achieve at least the challenged claims. *Id.*

VII. DISCRETIONARY FACTORS

A. 35 U.S.C. § 325(d) Does Not Favor Denial

The Board uses a two-part framework to analyze denial under 325(d):

> (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and
>
> (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, Paper 6 at 7 (PTAB Feb. 13, 2020). When considering the first prong, the PTAB considers the prosecution of the patent, and any post-issuance proceedings like *ex parte* reexams. *Id.* at 7-8. As to the second prong, the PTAB provided examples of "material errors," including whether the office overlooked a specific teaching of the relevant prior art or an error of law, such as misconstruing a claim term. *Id.* at n. 9. In *Advanced Bionics* the Board explained that the *Becton Dickinson* factors

are used within this framework to provide useful insight into how to apply each prong. *Id.* at 9.

With respect to the first prong, the '905 patent was issued over rejections in view of Hsu and Stanko[5]. None of the prior art in this petition were cited or addressed by either the Examiner or Applicant. This weighs in favor of institution. *See, e.g., Digital Check Corp. d/b/a ST Imaging v. E-Imagedata Corp.*, IPR2017-00178, Paper 6 at 12-13 (PTAB. April 25, 2017) (instituting where: "[T]here is no indication in the record that the Examiner rejected any claims based on either reference or that the Examiner or applicant substantively discussed either reference during prosecution[.]").

As discussed below, Scott, Lapsley, Robinson, Berardi, Shreve, and Kinoshita teach each and every element of the asserted claims. Accordingly, these references are also not cumulative of the art the Examiner considered.

B. 35 U.S.C. § 314(a) Does Not Favor Denial

The purpose of § 314(a) is to prevent serial petitions against the same patent, resulting in unnecessary harassment and wasted resources. *Celltrion, Inc. v. Genentech, Inc.*, IPR2018-01019, Paper 11 at 13 (PTAB Oct. 30, 2018) ("Celltrion filed a concurrent motion to join the Pfizer IPR, effectively ***obviating any***

[5] Although Shreve was cited in a later continuation of the same application resulting in US 10, 698,989, it was cited for in a different combination and regarding different limitations than those presented below. As such the inclusion of Shreve does not support denial under §325(D).

concerns of serial harassment and unnecessary expenditure of resources."). No other post-grant proceeding has ever been filed against the '905 patent. Accordingly, § 314(a) does not apply.

1. The *Fintiv* Factors Weigh in Favor of Institution

Likewise, the *Fintiv* Factors weigh in favor of institution:

A. *Fintiv* Factor 1: Whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted

The Court has not granted a stay, nor has a request for a stay been filed and it is unclear whether the Court would grant a stay in view of institution. Accordingly, this factor weighs in favor of institution.

B. *Fintiv* Factor 2: Proximity of the court's trial date to the Board's projected statutory deadline for a final written decision

The Court has not set a trial date. Based on recent cases that have gone to trial in front of Judge Albright, a trial date will likely be set 21-26 months from the filing of PO's complaint, *i.e.*, between December 2022 - May 2023:

- In *MV3 Partners LLC v. Roku, Inc.*, Case No. 18-cv-00308, a complaint was filed on October 16, 2018, and trial began October 5, 2020, with the Court entering a final judgment on December 21, 2020.

- In *ESW Holdings, Inc. v. Roku, Inc.*, Case No 19-cv-00044, the complaint was filed February 8, 2019, with trial beginning April 5, 2021. The final judgment issued August 24, 2021.
- In VLSI Technology LLC v. Intel Corporation, Case No. 21-cv-00299, the complaint was filed April 11, 2019, with trial beginning April 12, 2021. The final judgment has not issued to date.
- In *CloudofChange, LLC v. NCR Corporation*, Case No. 19-cv-00513, the complaint was filed August 30, 2019, with trial beginning May 17, 2021. The final judgment has not issued to date.

This petition is being filed on August 26, 2021. Thus, the approximate date of the PTAB hearing is February 2023. Accordingly, the PTAB trial will likely pre-date the district court trial, perhaps by several months. Accordingly, this factor weighs in favor of institution.

Even if the trial occurs shortly before the PTAB hearing, the PTAB has held that such close proximity of a district court trial date weighs in favor of institution. *See, e.g., MediaTek Inc. et al. v. Nippon Telegraph and Telephone Corp.*, IPR2020-01607, Paper 12 at 14 (PTAB April 2, 2021) ("*MediaTek*") (finding that Factor 2 weighed in favor of institution when that PTAB's decision was due within ***three months*** of the WDTX trial), *Western Digital Corp. et al. v. Martin Kuster*, IPR2020-01391, Paper 10 at 9 (PTAB February 16, 2021) ("*Western Digital*")

(finding Factor 2 weighed in favor of institution where "only a ***three-and-a-half month*** difference between the [WDTX] trial date and the due date for the final written decision"); *see also Facebook, Inc. v. USC IP Partnership, L.P.*, IPR2021-00034, Paper 13 at 11 (PTAB April 30, 2021) ("*USC IP*") (instituting IPR where the WDTX trial date was set ***five months*** before the Final Written Decision).

In any case, the proximity of a trial date is not dispositive in the *Fintiv* analysis: "[Factor 2] is not considered in isolation, but holistically along with other factors." *USC IP* at 11. Indeed, the PTAB has instituted IPR even where a district court trial is scheduled to occur ***five months*** before the PTAB's decision where, as here, the petition was filed in the early stages of litigation. *Id.*

Moreover, as discussed below, Petitioner has agreed not to pursue any grounds it raised or could have raised in the litigation. Likewise, this case is in its infancy with minimal investments made by the parties and the Court. Finally, the impact of the Delta variant of the COVID-19 virus has already begun to have a disruptive impact and may adversely impact case schedules as it did last year. Accordingly, this factor weighs in favor of institution.

C. *Fintiv* Factor 3: Investments in the parallel proceeding by the court and the parties

The district court litigation is in its infancy. Petitioner has not filed an answer. No discovery has taken place. Thus, there have been ***no*** investments, let alone significant investments, by the Court or the parties in this case related to

invalidity. Accordingly, this factor weighs in favor of institution. *USC IP* at 11 (finding the district court's earlier scheduled trial date of diminished importance where fact discovery had started less than two months before the petition was filed).

D. *Fintiv* Factor 4: Overlap between issues raised in the petition and the parallel proceeding

Petitioner further stipulates herein that, if this IPR proceeding is instituted, then Petitioner will not pursue in the Litigation the specific grounds identified above in connection with the referenced patents and claim.[6] *See* 35 U.S.C. §315(e)(2). This waiver eliminates any overlap in invalidity issues between the Litigation and an IPR instituted based on this Petition, and thus mitigates any concerns of duplicative efforts. *See, e.g., Sotera Wireless, Inc.* v. *Masimo Corporation*) as precedential. IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential) ("*Sotera*"); *Sand Revolution II, LLC v. Continental Intermodal Grp.-Trucking* LLC, IPR2019-01393, Paper 24 at 11-12 (PTAB June 16, 2020)

[6] This stipulation is not intended, and should not be construed, to limit Petitioner's ability to assert invalidity of the asserted claim of the '905 patent in the Litigation on any other ground (*i.e.*, invalidity under §§ 101, 112), regardless of whether *inter partes* review is instituted.

(informative) ("*Sand Revolution*"); *Google LLC et al v. Parus Holdings, Inc.*, IPR2020-00846, Paper 9 at 22 (PTAB October 21, 2020).

E. *Fintiv* Factor 5: Whether the petitioner and the defendant in the parallel proceeding are the same party

The petitioner here is the same party as the defendant in the district court case. While this factor may weigh slightly in favor of institution, it does not outweigh the remaining factors.

F. *Fintiv* Factor 6: Other circumstances that impact the Board's exercise of its discretion, including the merits

The merits of the petition also support institution. As discussed in more detail below, the prior art teaches each and every element of the challenged claims. Indeed, the challenged claims merely recite well known methods of cryptography that was known years before the '905 patent was filed. The Scott and Berardi references expressly disclose ID codes and biometric systems matching those claimed.

In addition, numerous prior art patents teach the same concept of using biometrics and device IDs in this cryptography context such as Scott and Berardi. Thus, the challenged claims merely recite the well-known concept of securing data or services with a biometric component and a device ID component which was known in the art years before the '905 patent was field. Accordingly, the

challenged claims should be held unpatentable. Accordingly, the merits of the petition weigh strongly in favor of institution.

VII. DETAILED EXPLANATION OF GROUNDS FOR INVALIDITY

As explained below pursuant to 37 C.F.R. §42.104(b), the cited prior art renders obvious the Challenged Claims of the '905 Patent. The cited references were not considered by the Patent Office during the examination of the '905 Patent.[7] The Challenged Claims are unpatentable based on each of the grounds presented below.

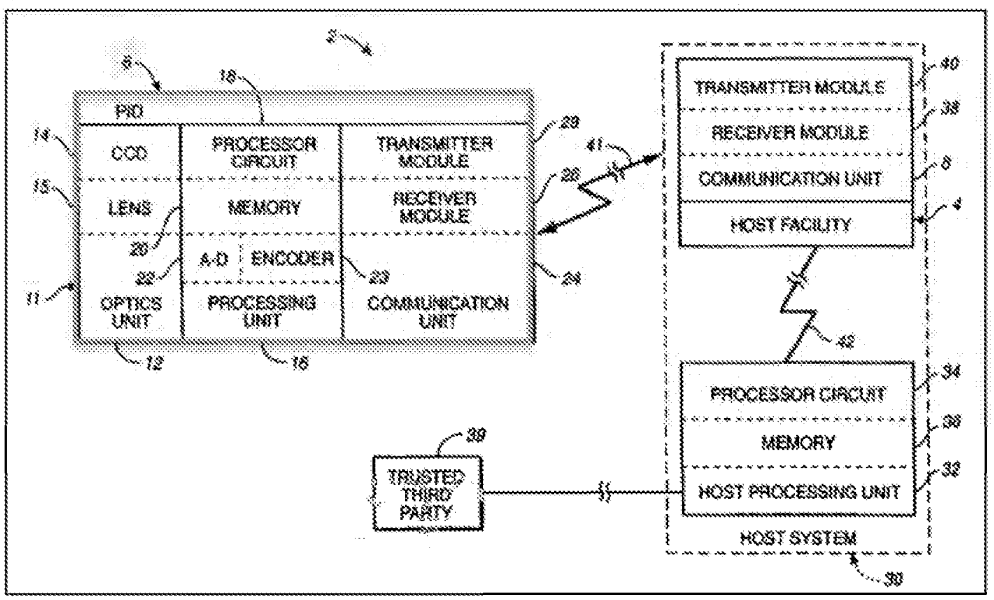
A. Ground 1: Claims 1, 3-10, and 12 are rendered obvious by Scott and Lapsley.

1. Claim 1

a) [1pre]: A method comprising:

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1005 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1E] *infra*.

[7] *See* Ex. 1001 at Face (References Cited).



Ex. 1005 at Fig. 1.

b) *[1A]: persistently storing biometric data of a legitimate user and an ID code on an integrated device;*

"persistently storing biometric data of legitimate user": Scott discloses storing biometric data of a user in memory 20 of the portable, hand-held PID 6. Ex. 1005 at 4:1-18 ("wherein the memory stores the biometric data"); *id.* at 11:11-20 ("Memory 20 also stores a fingerprint template that is generated by processing unit 16 from a fingerprint image signal provided by optics 12 unit when an individual first enrolls into PID 6 … [t]he fingerprint template is normally not changed once it is established in memory 20."), 15:30-16:6.

"***persistently storing … an ID code on an integrated device"***: Scott further discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including an ID code that uniquely identifies the PID 6. Ex.

1005 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including an ID code unique to the device, which may be set by the device manufacturer and can be the device serial number. Ex. 1005 at 11:11-13. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

c) *[1B]: responsive to receiving a request for a biometric verification of the user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;*

Scott discloses receiving a request for a biometric verification of the user by disclosing pressing a "verify" button on the PID 6, which can be a dedicated button such as the "#" button. Ex. 1005 at 16:19-29. Scott also discloses that in response to this request, the PID 6 can receive scan data from a biometric scan, such as a fingerprint scan from user placing a finger on platen 15 (see below), a voice biometric scan, "or any other type of biometric scan." *Id.* at 3:21-32.

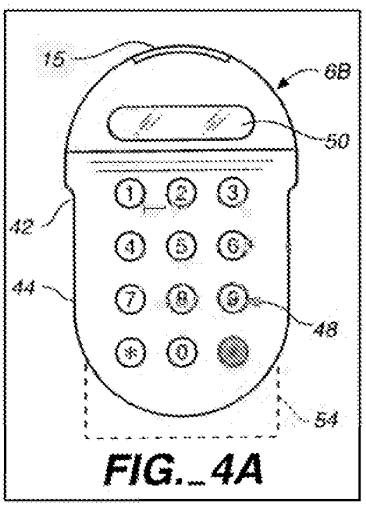


FIG._4A

Ex. 1005 at Fig. 4A.

d) *[1C]: comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;*

Scott discloses that after receiving the biometric scan data, the PID 6 compares the received biometric scan data (*e.g.*, voice, iris, or fingerprint biometric) to a stored biometric template in order to verify the user's identity. Ex. 1005 at 15:30-16:29.

e) *[1D]: responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,*

"responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code": Scott discloses that in response to determining that the biometric scan data matches the stored biometric data (*see* Claim [1C] *supra*), the PID 6 wirelessly transmits to a host facility 4 an encrypted

message with ID code and other data such as a synchronization counter. Ex. 1005 at 4:6-18, 5:22-6:24, 6:28-7:23 ("the access signal including an ID code associated only with the user device, button press information representing a requested function, and encrypted data encrypted with an encryption key associated with the user device, the encrypted data including a synchronization counter associated with the user device"), 12:14-18 ("Signals may be transmitted between PID 6 and host facility via any wireless transmission method."), 13:10-15, 19:30-32.

"for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority": Scott renders this limitation obvious by disclosing that a third-party trusted authority stores a list that includes an ID code and a public key for each registered PID 6.

Specifically, Scott discloses that the third-party trusted authority host processing unit 32 stores a list that includes an ID code and a public key for each registered PID 6. Ex. 1005 at 7:24-8:4, 8:18-22; 9:23-25, 11:12-13, 12:6-13, 19:18-20, Fig. 1. Upon receiving a device ID code from a PID 6, the host processing unit 32 compares it to the stored list to authenticate the transmitting PID 6 as a legitimately registered device. *Id.* at 5:10-21, 6:11-21; 13:10-15, 19:30-32 (authorizing synchronization data and encryption key). For example, the host processing unit 32 may receive an ID code signal associated with a PID 6,

determine that the PID 6 associated with the ID code belongs to a specific user, and provide access to a secure facility in response to verifying the PID 6. *Id.* at 7:24-8:4.

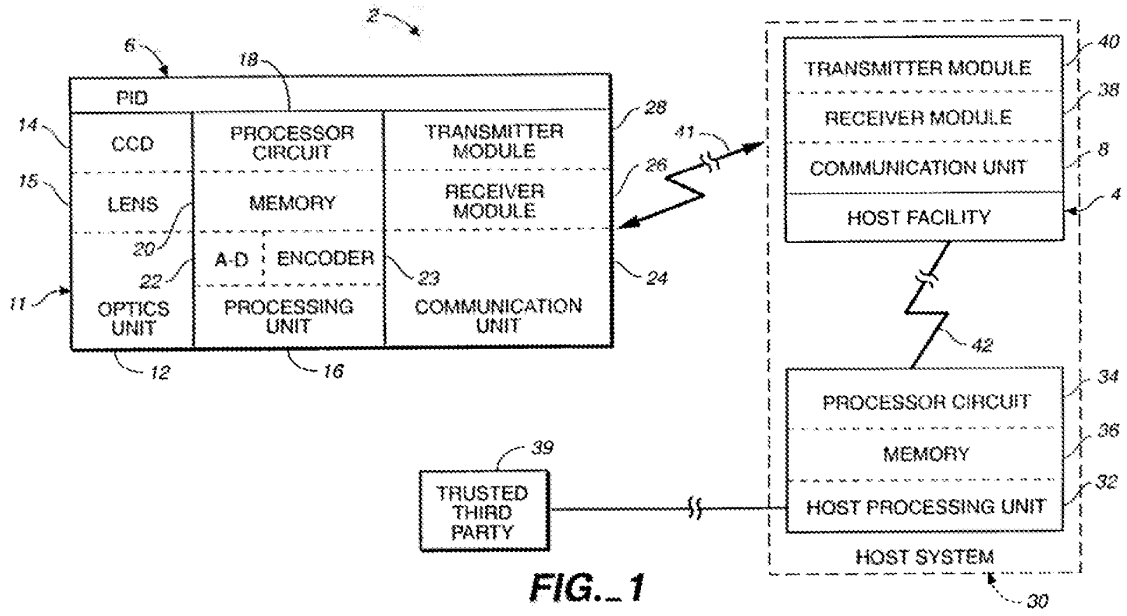


FIG._1

Id. at Fig. 1.

To the extent PO argues that Scott's host processing unit 32 is not a third-party trusted authority, Lapsley (US20010000535) provides additional disclosure rendering this feature of the limitation obvious to a POSITA. Lapsley discloses a third-party authentication system to validate a transaction initiated at a biometric device (*i.e.*, Party Identification Apparatus (PIA)). Ex. 1007 at Abstract, ¶54. The PIA includes a biometric sensor that receives a user's biometric input accompanying an electronic payment. *Id.* at ¶167. The PIA transmits the

biometric data and a PIA hardware identification code to a trusted third-party Data Processing Center (DPC). *Id.* at ¶168. The DPC includes a list of hardware identification codes for PIAs, wherein each respective code "makes the PIA uniquely identifiable to the DPC in all transmissions from that device." *Id.* at ¶¶85, 161. Using this list, the DPC identifies the PIA by its PIA hardware identification code. *Id.* at ¶¶85, 103, 104, 158, 166. Lapsley also discloses that communication security is achieved using an encryption scheme that uses public/private keys and admits such techniques are "well known in the industry." *Id.* at ¶82.

(1) **Motivation to Combine**

A POSITA would have been motivated to modify the authentication technique of Scott according to the teachings of Lapsley.

A POSITA would have been motivated to modify Scott's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique identify legitimate PIDs, as taught in Lapsley, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent. Ex. 1003 at ¶47. A POSITA would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction. Ex. 1007 at ¶¶8-9, 27, 29. A POSITA would have recognized Scott's examples of an ATM system, a store, or a bank as common security applications at

the time. Ex. 1005 18:29-19:20. A POSITA would have further understood that it was common to have an ATM that is not owned by a bank use the bank as a third party for authorization and it was common for a store to use a bank or credit card exchange as a third party for authorization. The disclosure of Scott welcomes this modification as seen by its disclosure of a Trusted Third Party 39 that stores encryption key credentials at a central location, thus providing a valuable service for "several host systems in a known manner." Ex. 1005 at 12:6-13, 17:17-19, Fig. 1.

f) [1E]: responsive to receiving an access message from the third –party trusted authority indicating that the thir-party trusted authority authenticated the ID code, allowing the user complete a financial transaction.

Scott discloses that in response to authentication of the received ID code by comparing it to a stored ID code, the receiver module 26 of PID 6 receives a random number signal from that enables access to a secure resource. Ex. 1005 at 17:20-18:19, 5:10-21, 8:5-12. The PID 6 is allowed access to an application (*e.g.*, key card entry, ATM, garage door, etc.) when the PID 6 sends a second transmission with the received random number signal sent from the host facility. *Id.* Specifically, Scott discloses after verification "the ATM (for example) commences normal operation" thus completing a financial transaction. *Id.*

2. Claim 3: *"[t]he method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."*

Scott discloses that after the PID 6 extracts a biometric trait of a user using a biometric sensor and compares that trait to a stored biometric trait, the PID 6 can transmit a verification signal "indicative of a successful verification of the user's identity." Ex. 1005 at 2:17-23, 7:24-8:4, 21:23-25, 22:6-23, 30:22-29; *see also* 20:3-9. Scott also discloses that the verification signal includes the ID code. *Id.* at 24:6-8.

3. **Claim 4:** ***"[t]he method of claim 1,*** *wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition"*

Scott discloses wherein the biometric data is a "unique identifier of a person," such as, for example, voice pattern, a fingerprint, or iris pattern. Ex. 1005 at 1:14-23, 2:5-16, 3:21-22 ("The biometric sensor system can include a fingerprint sensor, a voice sensor, or any other type of biometric sensor."), 15:30-16:6.

4. **Claim 5:** ***"[t]he method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."***

While Scott does not explicitly disclose the use of a mobile phone, Scott renders using a mobile phone obvious. Scott discloses a "portable, hand-held personal identification device" similar in size and shape to a cell phone. Ex. 1005 4:22-24, 8:23-24, 13:16-26; Ex. 1003 at ¶52. As well as the use of telephone lines and computer lines for communication with the PID 6. Ex. 1005 9:16-22. As such

a POSITA would have found it obvious to incorporate cellphone and other computer capabilities into the PID 6. Ex. 1003 at ¶52. Scott provides a motivation to do this as Scott teaches the PID should be small enough to be able to fit on a user's person while still providing access to a secure location. Ex. 1005 22:6-8. Combining a user's cellphone with the PID 6 would reduce what a user is required to carry while keeping the PID 6 small. Ex. 1003 at ¶52.

5. Claim 6: *"[t]he method of claim 1, wherein completing the financial transaction includes accessing an application."*

As explain in [1E], Scott discloses that in response to authentication of the received ID code by comparing it to a stored ID code, the receiver module 26 of PID 6 receives a random number signal from that enables access to a secure resource. Ex. 1005 at 17:20-18:19, 5:10-21, 8:5-12. The PID 6 is allowed access to an application (*e.g.*, key card entry, ATM, garage door, etc.) when the PID 6 sends a second transmission with the received random number signal sent from the host facility. *Id.*

6. Claim 7: *"[t]he method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."*

As explain in [1E] and [6], Scott discloses the PID 6 is allowed access to an application (*e.g.*, key card entry, ATM, garage door, etc.) when the PID 6 sends a

second transmission with the received random number signal sent from the host facility. *Id.*

7. Claim 8

a) [8A]: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and

Scott discloses receiving a request for the ID code by means of the PID 6 reaching a certain distance to a host facility's receiver module causing the PID's microprocessor to power up. Ex. 1005 at 17:20-18:4, Fig. 7; Ex. 1003 at ¶55. After receiving this request, Scott discloses that the PID 6 transmits the ID code to the host system. *Id.* As such the PID 6 determines the action does not require biometric verification. The host system requests, receives, and verifies the ID code before any biometric verification. *Id.* As illustrated in Figure 7 below, biometric verification occurs in step 118 (highlighted in yellow) after the host facility requests, receives, and verifies the ID code (steps highlighted in green)

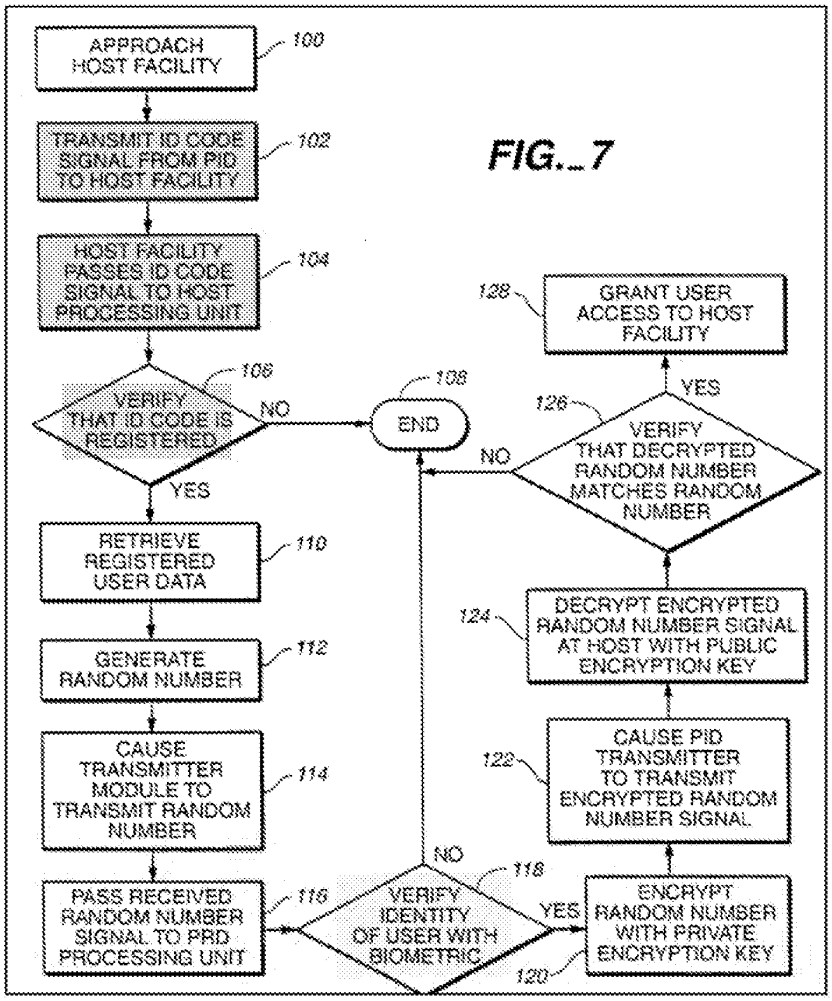


FIG._7

Id. at Fig. 7.

b) *[8B]: and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.*

As mentioned in [8A], Scott discloses that in response to the request from the host facility, the PID 6 sends the ID code without requesting scan data to confirm biometric match. Ex. 1005 at 17:20-18:4, Fig. 7; Ex. 1003 at ¶56.

8. Claim 9

a) [9pre]: An integrated device comprising:

Scott teaches that its disclosure is performed by a PID 6 to verify a user during authentication of the PID 6 provide secure access to protected resources such a hotel room or point of sale transaction. Ex. 1005 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* [1pre]-[1E] *supra*.

b) [9A]: a persistent storage media that persistently stores biometric data of a user and an ID code;

Scott discloses this limitation. Scott discloses that the recited data is written to the memory 20 of PID 6 in a tamper proof format that is unable to be subsequently altered. *See* claim [1A] *supra*; Ex. 1003 at ¶58.

c) [9B]:a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data,

"a verification unit in communication with the memory": Scott discloses a verification unit (*e.g.*, optics unit 12, platen 15, processor 16 (including A-D 22, encoder 23, and processor circuit 18), and notification light 324) in communication with the memory 20 of PID 6. Specifically, the optics unit 12 receives data from a user scan on platen 15 and transmits the biometrics data to memory 20 for comparison by the processor 16 to a stored biometric template. Ex. 1005 at 2:11-13, 11:5-7, 15:6-8, 16:19-29. Scott discloses that the processor 16 communicates directly with memory 20. *Id.* at 14:22-26. Scott further discloses that as part of the verification process, a PID can include a notification light 324 (*e.g.*, "a red light

emitting diode" or LED) that is activated upon the PID reaching a specific proximity to a transmitter of a host system for requesting the biometric scan. Ex. 1005 at 22:6-16. This notification light acts to begin the verification process and "prompt[s] the user to press (or swipe) a finger against a finger platen 322." *Id.* at 22: 11-16.

To the extent that Patent Owner argues that these mentioned elements are of distinct embodiments disclosed in Scott, a POSITA would have been motivated to, for example, combine the notification light 324 of the PID 320 described in Scott with the other PID 6 described in Scott, in order to better communicate context for verification of a user. Ex. 1003 at ¶60. A POSITA would also have a reasonable expectation that such a combination would be successful given that LED notifications were well-known at the time of the invention and that Scott already disclosed a PID embodiment that included one.

"receives scan data from a biometric scan for comparison against the biometric data": *See* claims [1C] and [1D] *supra*.

> *d) [9C]:a validation module… that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and*

See claims [1C]-[1E] *supra*. Scott discloses that the verification unit (*e.g.*, optics unit 12, platen 15, processor 16 (including A-D 22, encoder 23, and processor circuit 18), and notification light 324) wirelessly sends the data using a

communication unit 24 which includes a transmitter module 28 and a receiver module 26. Ex. 1005 at 4:6-18, 5:22-6:27, 6:28-7:23, 12:14-18; *see* claims [1C]-[1E] *supra*.

> *e) [9D]: responsive to the agent authenticating the one or more codes and the other data values,*

See claims [1D]-[1E] *supra*.

> *f) [9E]: a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to complete a financial transaction.,*

Scott discloses a radio frequency communicator (*e.g.*, communication unit 24 which includes a transmitter module 28 and a receiver module 26) that receives an access message from the agent allowing the user access to an application. *See* claim [1E] *supra*. Ex. 1005 at 17:20-18:19, 5:10-21, 8:5-12. . Specifically, Scott discloses after verification "the ATM (for example) commences normal operation" thus completing a financial transaction. *Id*.

9. **Claim 10:** *"The integrated device of claim 7[8], wherein the ID code is transmitted to the third-party trusted authority over a network."*

Scott discloses that the PID 6 wirelessly transmits an ID code and encryption data to a host facility over a wireless network, such as, for example, "the Internet or a private network." Ex. 1005 at 12:14-25, 4:6-18, 5:22-6:24, 6:28-7:23, 13:10-15, 19:30-32.

10. **Claim 12:** *"The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."*

See claims 5, 7 supra.

B. Ground 2: Claims 2 and 11 are rendered obvious by Scott, Lapsley, and Robinson.

1. Claim 2

Claim 2 recites "[t]he method of claim 1, further comprising: registering an age verification for the user in association with the device ID code." Scott discloses registering the device ID code of each PID 6. *See* claim [1D], *supra*.

However, Scott does not expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson (US2003/0177102) discloses that a central database 102 holds information related to users to authenticate a

[8] To the extent PO argues that claim 10, 11, or 12 are properly dependent on claim 9, the claims are still invalid. *See* Claim 9 supra. Petitioner takes no position in this proceeding regarding indefiniteness.

user's age to access an age restricted area, for example. Ex. 1008 at ¶¶27-28, 32, 66-67 Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user.

A POSITA would have been motivated to modify Scott to include registering an age verification for the user in association with the device ID code according to the teachings of Robinson. A POSITA would have been motivated to modify Scott's system such that an age verification for the user is registered in association with the device ID code, as taught in Robinson, to improve security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Scott's PID 6. Ex. 1008 at ¶9-10; Ex. 1003 at ¶64. The disclosure of Scott welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28.

2. Claim 10

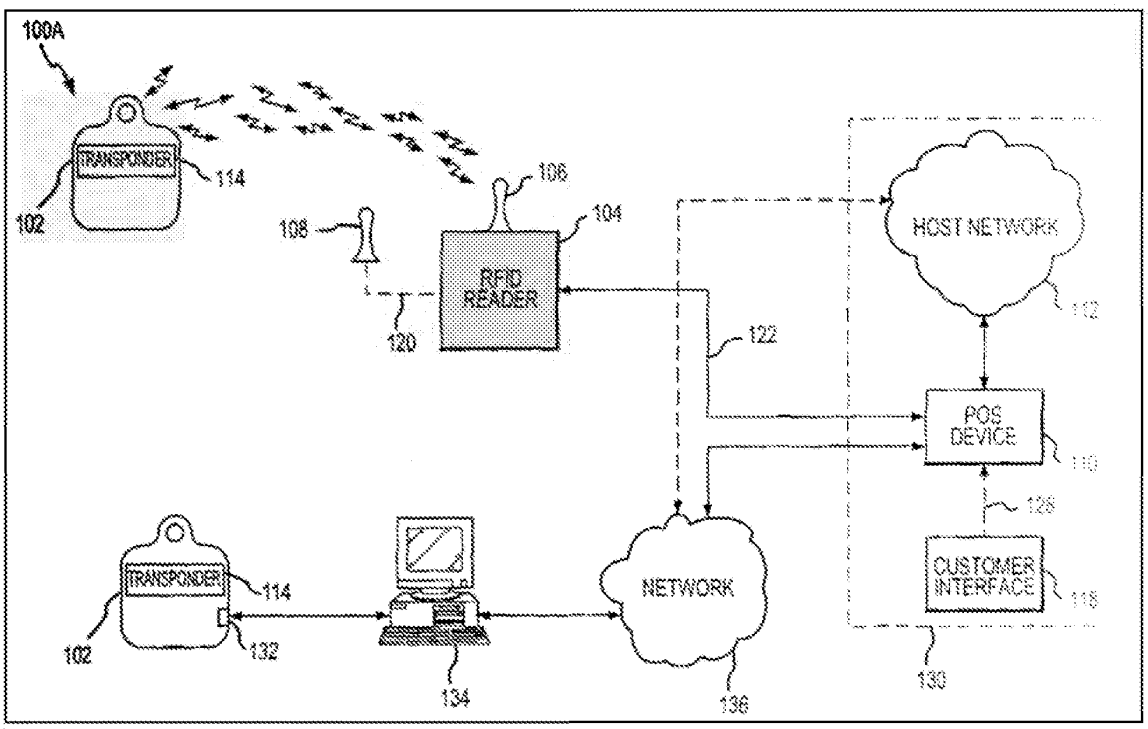
Claim 10 recites "[t]he integrated device of claim 7, wherein an age verification is registered in association with the device ID code." *See* Claim 3 *supra*.

C. Ground 3: Claim 1 and 3-7 are rendered obvious by Berardi, Shreve, and Kinoshita.

1. Claim 1

a) [1pre]: A method comprising:

Berardi discloses a method for verifying a user during authentication of an integrated device (*e.g.*, portable electronic Fob 102) that engages with RFID reader 104 to, for example, facilitate a point-of-sale transaction. Ex. 1010 at Abstract, 3:45-4:3, 12:36-48, Fig. 2; *see* claims [1A]-[1E] *infra*. The fob 102 is useful for completing a contactless transaction and would ordinarily be carried by a user for verification. Ex. 1010 at 1:15-18, 1:32-36.



Ex. 1010 at Fig. 2.

b) *[1A]: persistently storing biometric data of a legitimate user and an ID code on an integrated device;*

"persistently storing biometric data of legitimate user": Berardi discloses storing biometric data of a user in security database 212 of the portable fob 102 (a POSITA would understand that the database 212 can store multiple different things at the same time). Ex. 1010 at 28:50-65 ("The sensor fingerprint may be digitized and compared against a digitized fingerprint stored in a database (e.g., security database 212) included on fob 102.").

"***persistently storing … an ID code on an integrated device"***: Berardi further discloses that the fob 102 stores in database 214 a plurality of codes and

other data values including an account number unique to each fob which can include "unique fob serial number and user identification number," Track 1 and 2 data, and an unencrypted unique fob 102 identification code. Ex. 1010 at 10:64-11:12. Berardi also discloses that a unique fob identifier may be stored on database 212. *Id.* at 17:45-61.

> *c) [1B]: responsive to receiving a request for a biometric verification of the user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;*

Berardi discloses that the fob 102 includes biometric sensor and biometric membrane configured to activate the fob 102 when an accurate biometric signal is provided. Ex. 1010 at 12:36-41. For example, the user places a finger on the biometric sensor "to initiate the mutual authentication process between the fob 102 and the RFID read 104, or to provide secondary verification of the user's identity." *Id.* at 28:50-67. The scanned fingerprint data is then compared against stored data on fob 102 for authentication. *Id.*

> *d) [1D]: responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority,*

"responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code": Berardi discloses that in response to determining that the biometric scan data matches the stored biometric data, the fob

102 wirelessly transmits to RFID reader 104 (which transmits to POS Device 110/issuer system 1010) a message for authorization the includes fob identifying information which includes an account number unique to the fob, a unique fob serial number, user identification number, unique fob 102 identification code, and Track 1 and Track 2 data. Ex. 1010 at 10:56-11:12, 22:1-19, 28:50-67.

"for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority": Berardi renders this limitation obvious by disclosing that a third-party trusted authority (*e.g.*, issuer system 1010) stores a list that includes an ID code and a public key for each registered fob 102 and receives identifying information for each fob 102 for authorization. Ex. 1010 at 22:1-12. Berardi discloses that the issuer system 1010 includes an issuer account server (IAS) 1014 that processes fob identifying information. *Id.* at 22:20-41.

To the extent PO argues that Berardi fails to disclose this limitation, Shreve (US20020109580) provides additional disclosure rendering this feature of the limitation obvious to a POSITA. Shreve discloses a transceiver/fob device 12, which is "a remote keyless entry-based transceiver device," capable of two-way wireless communications with domain system 14 for secure access authorization based on biometrics. Ex. 1012 at Fig. 2a, ¶¶33, 35. Shreve discloses a service provider 24 with a secured database 31 that provides authentication of a transaction

initiated by a fob device 12. *Id.* at ¶39. For authentication, the database 31 contains cross-references between "the key fob ID and other user specific information (e.g., accounts, access privileges, biometrics, etc) that can be used by the authentication algorithm **23** to further facilitate the authentication process." *Id.* at ¶39, claim 47.

(1) **Motivation to Combine**

A POSITA would have been motivated to modify Berardi's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique identify legitimate fob devices, as taught in Shreve, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent and to provide an additional level of security during authentication. Ex. 1003 at ¶78. A POSITA would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction. Ex. 1012 at ¶6.

> *e) [1E]: responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority authenticated the ID code, allowing the user complete a financial transaction.*

Berardi discloses that in response to authentication of the received identifying information of the fob 102, the POS device 110 may send "an optical

and/or audible transaction status message" to the RFID reader 104 for communication directly with the customer. *Id.* at 20:51-62, Fig. 8.

To the extent PO argues that Berardi fails to disclose this limitation, Kinoshita (US20030055792) provides additional disclosure rendering this feature of the limitation obvious to a POSITA. Kinoshita discloses a portable device 14 that authenticates a user before transmitting a user ID to a POS terminal 11, which forwards the user ID to a third-party payment gateway 15 to authorize a payment transaction. Ex. 1013 at ¶¶168-69, Fig. 1. Specifically, the payment gateway 15 confirms the authenticity of the portable device 14 by comparing the device ID of the portable device 14 to stored device ID in a user table 154a. *Id.* at ¶171. After the payment gateway 15 receives a user ID and a request for transaction, the payment gateway 15 sends an e-mail message that includes commands for direction of payment to be executed by the portable device 14. ¶¶168-69. Upon receiving the e-mail message, the portable device 14 "executes an application for payment according to the commands included in the e-mail." *Id.* at ¶¶168-69, 179-83.

Kinoshita further discloses that the secure resource can include, for example, computer software such as a payment application. Ex. 1013 at ¶¶168-69, 179-83.

(1) **Motivation to Combine**

A POSITA would have been motivated to modify Berardi's system such that responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, as taught in Kinoshita, to improve security of the system by consolidating ID codes to a central location at a secure third-party agent and to provide an additional level of security during authentication. Ex. 1003 at ¶82. A POSITA would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction and to initiate access from a secure entity. Ex. 1013 at ¶5; Ex. 1003 at ¶82.

2. **Claim 3:** *"[t]he method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."*

Scott discloses that after the PID 6 extracts a biometric trait of a user using a biometric sensor and compares that trait to a stored biometric trait, the PID 6 can transmit a verification signal "indicative of a successful verification of the user's identity." Ex. 1005 at 2:17-23, 7:24-8:4, 21:23-25, 22:6-23, 30:22-29; *see also* 20:3-9. Scott also discloses that the verification signal includes the ID code. *Id.* at 24:6-8.

3. **Claim 4:** ***"[t]he method of claim 1,*** *wherein the biometric data includes data from one or more of a fingerprint, palm print, a*

retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition"

Berardi discloses wherein the biometric data may include "the digital reading of a fingerprint, thumbprint, or the like." Ex. 1010 at 12:36-41. A POSITA would understand Berardi to teach use of any biometric, including any of a palm print, retinal scan, iris scan, hand geometry, facial recognition, signature recognition and a voice recognition. Ex. At 1003 at ¶4.

4. **Claim 5:** ***"[t]he method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."***

Berrardi discloses an integrated device portable fob 102 comprising a "wristwatch, keychain, cell phone, etc." Ex. 1010 at 4:4-10.

5. **Claim 6:** ***"[t]he method of claim 1, wherein completing the financial transaction includes accessing an application."***

As explain in [1E], Berardi discloses that in response to authentication of the received identifying information of the fob 102, the POS device 110 may send "an optical and/or audible transaction status message" to the RFID reader 104 for communication directly with the customer. *Id.* at 20:51-62, Fig. 8.

To the extent PO argues that Berardi fails to disclose this limitation, Kinoshita (US20030055792) provides additional disclosure rendering this feature of the limitation obvious to a POSITA. Kinoshita discloses a portable device 14 that authenticates a user before transmitting a user ID to a POS terminal 11, which

forwards the user ID to a third-party payment gateway 15 to authorize a payment transaction. Ex. 1013 at ¶¶168-69, Fig. 1. Specifically, the payment gateway 15 confirms the authenticity of the portable device 14 by comparing the device ID of the portable device 14 to stored device ID in a user table 154a. *Id.* at ¶171. After the payment gateway 15 receives a user ID and a request for transaction, the payment gateway 15 sends an e-mail message that includes commands for direction of payment to be executed by the portable device 14. ¶¶168-69. Upon receiving the e-mail message, the portable device 14 "executes an application for payment according to the commands included in the e-mail." *Id.* at ¶¶168-69, 179-83.

6. Claim 7: *"[t]he method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."*

As explain in [1E] and [6], Kinoshita discloses that the secure resource can include, for example, a payment application. Ex. 1013 at ¶¶168-69, 179-83.

7. Claim 9:

a) [9pre]: An integrated device comprising:

Berardi teaches that its disclosure is performed by an integrated device (*e.g.*, portable electronic Fob 102) that engages with RFID reader 104 to, for example, facilitate a point-of-sale transaction. Ex. 1010 at Abstract, 3:45-4:3, 12:36-48, Fig. 2; *see* [1pre]-[1E] *supra*.

b) *[9A]: a persistent storage media that persistently stores biometric data of a user and an ID code;*

Berardi discloses this limitation. Berardi discloses storing the recited data of a user in security database 212 of the portable fob 102 (a POSITA would understand that the database 212 can store multiple different things at the same time). *See* claim [1A] *supra*; Ex. 1003 at ¶90.

c) *[9B]:a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data*

"a verification unit in communication with the memory": Berardi discloses a verification unit (*e.g.*, biometric sensor 904, protocol controller 208, authentication circuit 210) in communication with database 214. Specifically, the sequence controller 208 may be in communication with database 214 and biometric sensor 904. Ex. 1010 at 8:11-26; 18:55-19:36, Fig. 9.

"receives scan data from a biometric scan for comparison against the biometric data": *See* claims [1C] and [1D] *supra*.

d) *[9C]:a validation module ... that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and*

See claims [1C]-[1E] *supra*. Berardi discloses that the verification unit (*e.g.*, biometric sensor 904, protocol controller 208, authentication circuit 210) wirelessly sends the data using a transponder (antenna 202, RF I/F 204,

modulator/demodulator 206). Ex. 1010 at 7:4-33, 11:55-12:25; *see* claims [1C]-[1E] *supra*.

> *e) [9D]:responsive to the agent authenticating the one or more codes and the other data values,*

See claims [1D]-[1E] *supra*.

> *f) [9E]:a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction.,*

Berardi in light of Kinoshita discloses a radio frequency transponder (antenna 202, RF I/F 204, modulator/demodulator 206) that receives an access message from the agent allowing the user access to an application. Ex. 1010 at 7:4-33, 11:55-12:25; Ex. 1013 at ¶¶168-69, Fig. 1; *see* claim [1D], [1E] *supra*.

8. **Claim 10:** "*The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.*"

Berardi discloses that the fob 102 wirelessly transmits identifying information to RFID reader 103 over a wireless network, such as, for example, the Internet. Ex. 1010 at 2:32-36, 7:28-35.

9. **Claim 12:** "*The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.*"

See claims 5, 7 supra.

VIII. SECONDARY CONSIDERATIONS

At this stage of these proceedings, Petitioner has no burden to identify and rebut secondary considerations. Rather, Patent Owner must first present a *prima facie* case for such consideration, which Petitioners should then have the chance to rebut. *Sega of Am., Inc. v. Uniloc USA, Inc.*, IPR2015-01453, at *10 (Mar. 10, 2015). The Board typically rejects arguments against institution based on objective indicia, so that the Petitioners can have a fair opportunity to address any secondary indicia evidence on reply. *Petroleum Geo-Services Inc. v. WesternGeco LLC*, IPR2015-01478, at *22 (Mar. 17, 2015); Ex. 1003, ¶ 119; Ex. 1003 ¶ 141.

IX. CONCLUSION

For at least the foregoing reasons, the instant petition should be instituted.

Respectfully submitted,

Date: August 26, 2021

/s/ Marissa Ducca
Marissa Ducca (Reg. No. 59,807)

CERTIFICATION UNDER 37 C.F.R. § 42.24

Under the provisions of 37 C.F.R. § 42.24, the undersigned hereby certifies that the word count for the foregoing Petition for *inter partes* review (excluding the table of contents, table of authorities, mandatory notices, certificate of service or word count, and appendix of exhibits or claim listing) totals 10,823 words, which is less than the 14,000 words allowed under 37 C.F.R. § 42.24(a)(i).

Date: August 26, 2021

/s/ Marissa Ducca
Marissa Ducca (Reg. No. 59,807)

CERTIFICATE OF SERVICE (37 C.F.R. §§ 42.6(E), 42.105(A))

The undersigned hereby certifies that on August 26, 2021 two copies of this petition and supporting exhibits were served on counsel of record at the mailing address below via Federal Express Standard Overnight mail, and a courtesy copy was served via email on litigation counsel at the email address below:

Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City UT 84107

dhecht@hechtpartners.com
mprice@hechtpartners.com
emcdonough@hechtpartners.com
wwu@hechtpartners.com
jzak@hechtpartners.com
erobinson@porterhedges.com

Date: August 26, 2021

By: */s/ Marissa Ducca*
Marissa Ducca (Reg. No. 59,807)
QUINN EMANUEL URQUHART & SULLIVAN LLP
1300 I St. NW
Washington, DC 20005
Email: marissaduca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

Counsel for Petitioner Samsung

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC, *Plaintiffs*, v. SAMSUNG ELECTRONICS, CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC, *Defendants*.	Civil Action No. 6.21-CV-00210 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendants Samsung Electronics Co., Ltd. ("SEC") and Samsung Electronics America, Inc. ("SEA") (collectively, "Samsung" or "Defendants"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Samsung infringes one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. Upon information and belief, SEC is a corporation organized under the laws of the Republic of Korea, having a place of business at 129, Samsung-Ro, Yeongtong-Gu, Gyeonggi,

16677, Republic of Korea. SEC may be served with process pursuant to Federal Rule of Civil Procedure 4(f)(1).

4. Upon information and belief, SEA is a corporation organized under the laws of New York, having a principal place of business at 85 Challenger Rd., Ridgefield Park, NJ 97660. SEA maintains a place of business in this District at 12100 Samsung Blvd., Austin, TX 78754. SEA may be served with process through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201.

5. SEC designs, manufactures, and provides to the United States and other markets a wide variety of hardware and software products and services, including consumer electronics, mobile phones, handheld devices, tablets, laptops and other personal computers, storage devices, televisions, and electronic devices.

6. Upon information and belief, SEA is a wholly-owned subsidiary of SEC and is responsible for domestic distribution of Samsung's consumer products, including the products accused of infringement herein.

JURISDICTION AND VENUE

7. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

8. This Court has personal jurisdiction over Samsung because it has conducted and continues to regularly conduct business within the State of Texas and this District. Samsung has purposefully and voluntarily availed itself of the privileges of conducting business in the United States, the State of Texas, and this District by continuously and systematically placing goods into

the stream of commerce through an established distribution channel with the expectation that they will be purchased by consumers in this District. Samsung directly and/or through intermediaries (including distributors, sales agents, and others), ships, distributes, sells, offers to sell, imports, advertises, makes, and/or uses its products (including but not limited to the products accused of infringement herein) in the United States, the State of Texas, and this District.

9. SEA is registered to do business in Texas and maintains an agent for service of process in Texas. SEA maintains places of business within the Western District of Texas, including at 12100 Samsung Blvd., Austin, TX 78754.

10. Upon information and belief, Samsung has authorized retailers that offer and sell products on its behalf in this District, including products accused of infringement herein. Upon information and belief, these include Walmart, *e.g.*, Supercenter #939, 4230 Franklin Ave., Waco, TX 76710; Target, *e.g.*, at 5401 Bosque Blvd., Waco, TX 76710; Best Buy, *e.g.*, at 4627 S. Jack Kultgen Expy., Waco, TX 76706; T-Mobile Store, *e.g.,* at 1107 N Valley Mills Dr., Bldg 1, Waco, TX 76710; and Verizon, *e.g.*, at 1820 S Valley Mills Dr., Waco, TX 76711, among many others.

11. Proxense's causes of action arise directly from Samsung's business contacts and other activities in the State of Texas and this District.

12. Samsung has derived substantial revenues from its infringing acts within the State of Texas and this District.

13. Venue is proper in this District as to SEC pursuant to 28 U.S.C. § 1391(c)(3) because it is not a resident of the United States and may therefore be sued in any judicial district.

14. Venue is proper in this District as to SEA pursuant to 28 U.S.C. § 1400(b) because SEA has committed acts of infringement in this District and has regular and established places of business in this District.

15. Joinder of SEC and SEA is proper because they are related entities that are either jointly and severally liable for infringement, or that make, use, sell, offer to sell, and/or import the same or similar products accused of infringement herein. Further, upon information and belief, SEC and SEA use the same underlying hardware and/or software in their infringing products and therefore the factual question of infringement will substantially overlap between SEC and SEA. Proxense anticipates there will be substantial overlap with respect to discovery.

16. Samsung has committed acts of infringement in this District and does business in this District, including making sales and/or providing service and support for customers and/or end-users in this District. Samsung purposefully and voluntarily sold one or more infringing products with the expectation they would be purchased in this District. These infringing products have been and continue to be purchased in this District. Thus, Samsung has committed acts of infringement within the United States, the State of Texas, and this District.

PATENTS-IN-SUIT

17. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 1**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=08352730.

18. On March 26, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,298,905 (the "905 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 905 Patent is attached hereto as **Exhibit 2**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09298905.

19. On June 30, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,698,989 (the "989 Patent") entitled "Biometric personal data key (PDK)

authentication." A true and correct copy of the 989 Patent is attached hereto as **Exhibit 3**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=10698989.

20. On June 2, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,049,188 (the "188 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 188 Patent is attached hereto as **Exhibit 4**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09049188.

21. On January 12, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,235,700 (the "700 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 700 Patent is attached hereto as **Exhibit 5**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09235700.

22. Proxense is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the 730, 905, 989, 188, and 700 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

23. The technologies of the Patents-in-Suit were invented by John Giobbi and David L. Brown. The 730 and 905 Patents generally cover systems and methods for an integrated device that persistently stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (*e.g.*, a finger-print) can be compared against the stored biometric data. Once the user has been biometrically verified by the integrated device, a code can be wirelessly

transmitted for authentication. The 989 Patent generally covers systems and methods of verifying a user during authentication of an integrated device.

24. The 188 and 700 Patents generally covers a hybrid device including a personal digital key ("PDK") and receiver-decoder circuit ("RDC"), wherein the PDK and RDC are coupled for communication with each other. The 188 and 700 Patents also includes a number of system configurations for use of the hybrid device including: use of the hybrid device in a cell phone; simultaneous use of the PDK and the RDC functionality of hybrid device; use of multiple links of hybrid device to generate an authorization signal, use of multiple PDK links to the hybrid device to generate an authorization signal; and use of the hybrid device for authorization inheritance.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

25. Global contactless transaction values were estimated at $2 trillion in 2020. By 2024, they may reach $6 trillion according to forecasts. Mobile payments, or transactions initiated on mobile devices such as cell phones or tablet computers, have become increasingly popular as applications like Samsung Pay, launched in 2015, come bundled with Samsung's popular devices, like the Galaxy-branded line of phones. According to Samsung, "consumers have relied on Samsung Pay to make billions of transactions." Mobile payments can include payments for goods and services purchased over the internet (*e.g.,* through merchant websites or applications), or payments at a point of sale, which are payments initiated from a mobile device at a physical location.

26. Near Field Communication ("NFC") is a form of contactless communication between devices that allows two NFC-equipped devices placed within a few centimeters of each other to exchange data. NFC technology provides power consumption and ease-of-use advantages

as compared to other methods of close-proximity wireless communication (*e.g.*, Bluetooth). NFC can be used to facilitate mobile payments when an NFC-equipped device (such as a smartphone or electronic wearable like a watch) is placed near a contactless merchant terminal, allowing the devices to exchange payment data.

27. Contactless merchant terminal adoption in the U.S. has been expedited by card issuer security requirements. Card issuers in the United States set an October 2015 deadline for merchants to upgrade payment terminals capable of accepting credit cards with embedded chips for security, and many of these upgraded terminals have NFC capability built in. In December 2015, approximately 2.36 million contactless terminals were in service in the United States. As a result of the COVID-19 pandemic, there has been a sharp rise in adoption of contactless payment all over the globe.

28. Magnetic Secure Transmission ("MST") is a technology that emits a magnetic signal to mimic the magnetic strip on a traditional payment card. MST technology can be used to facilitate mobile payments when an MST-equipped device is placed near a merchant terminal, allowing the devices to exchange data. MST does not generally require merchants to upgrade payment terminal software or hardware. The technology was developed to facilitate contactless payments on point-of-sale terminals that can accept only conventional magnetic stripe cards. LoopPay, a contactless payments company that utilized MST (and was acquired by Samsung), claimed a 90% merchant acceptance rate.

II. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

29. Proxense was founded in 2001 as a limited venture. The company was formally incorporated in 2005 as an LLC. From approximately 2004-2012, Proxense developed, *inter alia*, mobile payment technologies and commercial products, employing over thirty engineers, and

investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

30. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of utilizing small electronic sensors, or receiver-decoder circuits ("RDCs"), capable of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

31. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including three of the asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

32. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 6**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), **Exhibit 7**.

33. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), Exhibit **8**. The DARKReading article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

34. It would be years until products like Apple Pay (2014) and Samsung Pay (2015) were launched and became mainstream; Apple's TouchID, which involves fingerprint recognition technology, and Samsung's fingerprint scanner on its own phones, were introduced in 2013 and 2014, respectively. Accordingly, Proxense's technology was years ahead of the industry.

35. After the launch of services like Samsung Pay, and its inextricable link to the some of the most popular smartphone hardware devices in the United States, and the world, Proxense

would find itself unable to compete with companies like Samsung, even though Proxense invented the technology utilized in these solutions.

36. Today, Proxense holds at least 65 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management and mobile payments. Proxense continues to prosecute new patents on its proprietary technology.

III. INFRINGEMENT ALLEGATIONS

1. Proxense's Interactions with Samsung

37. In or around April 2017, Proxense was introduced to Samsung. Since at least that time, Samsung has had constructive notice of the Patents-in-Suit and the scope of their claims as of at least their dates of issue. Proxense has given Samsung actual notice of the Patents-in-Suit, and also placed Samsung on notice of the Patents-in-Suit as of the date of public filing of this Complaint.

38. Samsung has also had knowledge of the infringing nature of its activities, or at least a willful blindness regarding the infringing nature of its activities, since at least Proxense's making Samsung aware of the Patents-in-Suit, if not as of the public filing of this Complaint.

39. Despite Samsung's knowledge of the Patents-in-Suit, and its constructive knowledge of its infringing actions, Samsung continued to infringe the claims of the Patents-in-Suit. Samsung's infringement has been and continues to be willful since at least the date of the public filing of this Complaint.

2. The Accused Products

40. Samsung has manufactured, used, marketed, distributed, sold, offered for sale, and exported from and imported into the United States devices and software that directly and/or

indirectly infringe (literally or via the doctrine of equivalents) the Patents-in-Suit. Samsung has distributed variants of Samsung Pay that have included functionality to verify a user during authentication of a smartphone. Samsung Pay is operable on a range of Samsung devices, including at least all smartphones from the Galaxy S6 and above, including but not limited to, at least the Samsung devices set forth in **Appendix A**, including Galaxy S21, S20+, S21 Ultra, Galaxy S20, S20+, S20 Ultra 5G, Galaxy Fold, Galaxy Z-Flip, ZFlip 5G, Galaxy Note 20, Note 20 Ultra, Note10, Note10+, Note10+ 5G, Note5, Galaxy S10e, S10, S10+, Galaxy Note9, Galaxy S9, S9+, Galaxy Note8, Galaxy Note5, Galaxy S8, S8+, Galaxy S7, S7 edge, Galaxy S6, S6 edge, S6 edge+, S6 Active, Galaxy A90, Galaxy A80, Galaxy A70, A71, A71 5G, Galaxy A50, A51, Galaxy A40, Galaxy A30, A31, Galaxy A20e, Galaxy A8, Galaxy A7, Galaxy A5, Galaxy J7, Galaxy J5 Pro, Galaxy Watch S3, Galaxy Watch S2 Sport, Galaxy Watch S2 Classic, Gear S3 Frontier, Gear S3 Classic, Galaxy Watch Active 2, Galaxy Watch Active, Galaxy Watch, Gear Sport, Gear S3, and Gear S2, and all Samsung devices released since September 2015. The current and previous versions of Samsung Pay and devices with Samsung Pay, alone and together, are non-limiting instances of the Accused Products. The Accused Products practice the claims of the Patents-in-Suit to improve the shopping experience of their users, and to improve Samsung's position in the market.

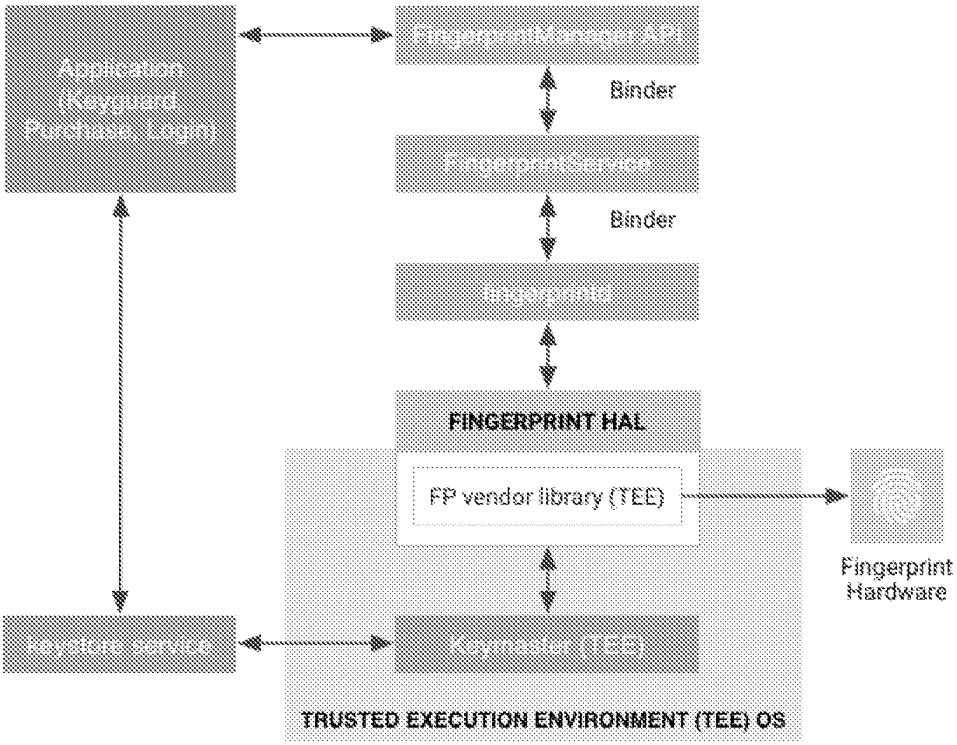
3. Samsung's Infringement of the Patents-in-Suit

41. Samsung Pay is described by Samsung as "an easy way to make purchases on your phone or watch." "It turns your device into a digital wallet that carries credit, debit, or gift cards." "And don't worry, you can use biometric security, so no one can access your financial data." Samsung advertises that "Samsung Pay is only available on select phone and watch models" and

that Samsung Pay may be used on a smart watch with a non-Samsung phone running Android 6.0 or later. **Exhibit 9 (Set up Samsung Pay on your phone, Samsung Support)**.

42. On information and belief, Samsung phones utilize Android's Fingerprint Hardware Interface Definition Language ("HIDL") to connect to its vendor-specific library and fingerprint hardware (e.g., a fingerprint sensor); to implement the Fingerprint HIDL, Samsung implements IBiometricsFingerprint.hal (the "Fingerprint HAL") in its vendor-specific library. Biometric data is protected because fingerprint templates must be signed with a private, device-specific key under the Fingerprint HIDL implemented by Samsung.

43. Fingerprint HAL interacts with Keystore Application Programming Interface ("API") and Keymaster components which provide hardware-backed cryptography for secure key storage in a secure environment, such as the Trusted Execution Environment ("TEE"). A high-level data flow for fingerprint authentication is produced below:

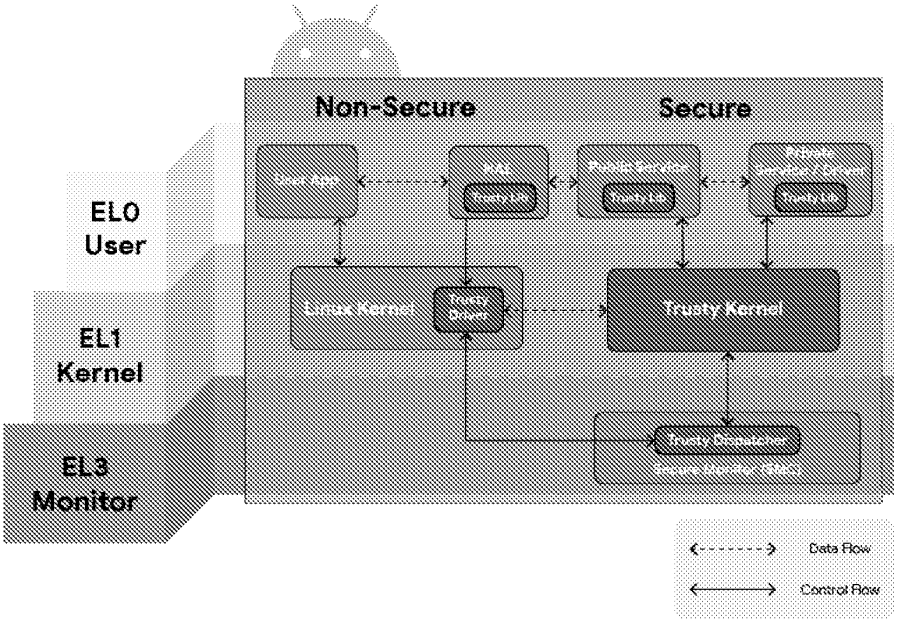


44. Keymaster functions include private key operations (*e.g.*, KeyPurpose:DECYPT and KeyPurpose::SIGN), e.g. a secret decryption value.

45. The Fingerprint HAL guidelines are described in the Android documentation as being designed to ensure that fingerprint data is not leaked and is removed when a user is removed from a device: Raw fingerprint data or derivatives (for example, templates) must never be accessible from outside the sensor driver or TEE. If the hardware supports a TEE, hardware access must be limited to the TEE and protected by an SELinux policy. The Serial Peripheral Interface (SPI) channel must be accessible only to the TEE and there must be an explicit SELinux policy on all device files. Fingerprint acquisition, enrollment, and recognition must occur inside the TEE.

46. "Trusty" is a secure Operating System ("OS") that provides a Trusted Execution Environment for Android, the operating system run on Samsung's smartphone devices. On information and belief, on Samsung's smartphone products, the Trusty OS runs on the same processor as the Android OS, and the two OS's run parallel to each other. Trusty has access to the full power of a device's main processor and memory but is completely isolated from the rest of the system by both hardware and software. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android.

47. On ARM systems, like Samsung's devices, Trusty uses ARM's Trustzone™ to virtualize the main processor and create a secure TEE. An overview diagram of Trusty is reproduced below:



48. Uses for a TEE like Trusty include mobile payments, secure banking, multi-factor authentication, device reset protection, replay-protected persistent storage, and secure PIN and fingerprint processing.

49. Samsung describes that "[w]ith Samsung Pay, each transaction is covered by your bank's fraud protection and authenticated by your fingerprint, PIN or iris scan." "Plus, Samsung Knox and tokenization add extra layers of security." See **Exhibit 10 (Samsung Pay Website)**.

50. According to Samsung, Samsung Pay uses three levels of security to enable secure payments: fingerprint or iris-scanning authentication, tokenization and Samsung Knox, Samsung's defense-grade mobile security platform.

51. Samsung Knox "builds upon the Android Keystore by providing a tamper-proof, detection-based lock-down of cryptographic keys." On Samsung devices utilizing Knox, "the authentication software doesn't share or distribute the biometric measurements of any user." **Exhibit 11** (Knox Platform for Enterprise, Version 1.3.1 (2020)), page 41. "The measurements are stored in a format that can't be used to reproduce the original biometric, and can only be

accessed and decoded within the specific part of the TrustZone that has access to the biometric hardware." *Id.*

52. Visa has described Samsung Pay as "a simple way for customers to pay that meets all 2015 EMV security standards." *See* **Exhibit 12 (Visa and Samsung Pay)** . EMV, which originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard, is a payment method based upon a technical standard for smart payment cards and for payment terminals and automated teller machines which can accept them.

53. EMVCo, LLC ("EMVCo") facilitates worldwide interoperability and acceptance of secure payment transactions. EMVCo is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders, including Samsung. EMVCo manages and evolves the EMV Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Samsung has received approval for the accused products as EMV Contactless Level 1 Mobile Products, *e.g.*, recently for the Samsung Galaxy S21 5G, Product Name SM-G991U. The publicly available approval letters, attached hereto as **Exhibit 13**, describe that EMVCo received a request for approval and found reasonable evidence that the submitted samples sufficiently conform to the EMV Contactless Interface Specification and other EMVCo requirements. Notably, EMV specifications were first published in 2007, years after the priority dates of all of the Patents-in-Suit.

54. One means of promoting payment security is "tokenization," an approach that substitutes sensitive data like account numbers and other personally identifiable information with a non-sensitive equivalent that has no intrinsic or exploitable meaning or value.

55. EMV payment tokens are open-loop tokens provisioned by a token service provider ("TSP"). Like other tokens, EMV payment tokens are used to replace the actual payment credential (*e.g.*, primary account number "PAN") with another numeric value.

56. The U.S. Payments Forum (formerly the EMV Migration Forum) is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of and enhance opportunities for payment transactions. According to the U.S. Payments Forum, Samsung was "among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases."

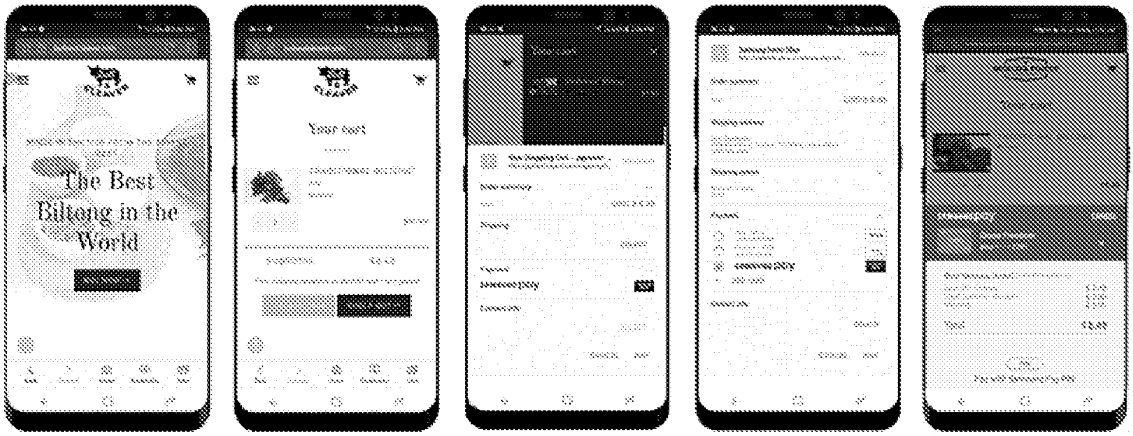
57. On information and belief, EMV payment tokens are issued to Samsung Pay equipped devices in exchange for a credit card number by a TSP such as Visa, Mastercard, American Express or Discover. On information and belief, device-specific payment tokens are stored by Samsung Pay-equipped devices.

58. The device-specific EMV payment tokens may be stored in three locations, one of them being a secure element / integrated circuit card ("ICC"). The first Samsung Pay-equipped devices, the Galaxy S6 and S6 Edge included a security cryptocontroller, *e.g.*, the Infineon SLE 97 ICC; on information and belief, subsequent devices equipped with Samsung Pay continued to use ICC elements. Secure elements like Infineon's SLE ICC are, according to the U.S. Payments Forum, "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

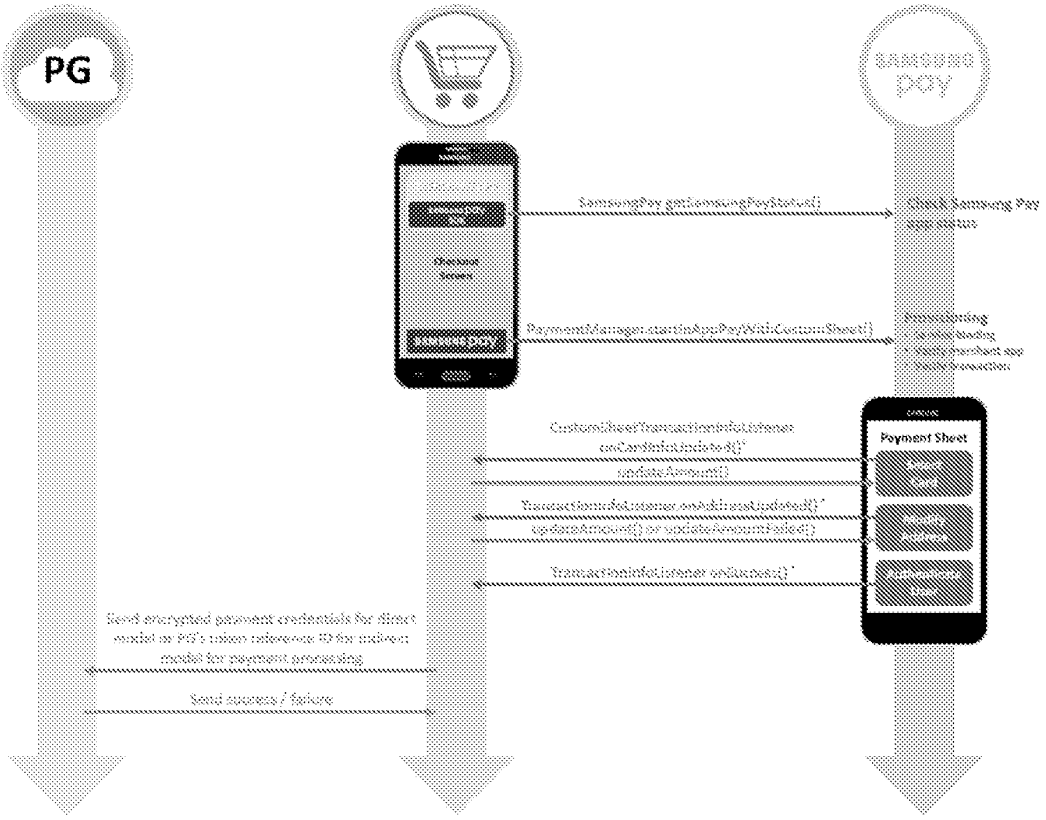
59. Samsung Pay requests biometric verification before providing payment credentials to merchants. The location/type of the purchase determines how the request is initiated.

60. For example, integrating the Samsung Pay API into their websites permits a merchant to accept Samsung Pay. When implemented via integration of the Samsung Pay API,

"the user initiates checkout, selects Samsung Pay as the preferred payment method, authenticates with a fingerprint or PIN, and voila — payment complete." Samsung further describes that "[w]hen properly implemented, the API also supports editing the billing/shipping address in Samsung Pay and selecting a different enrolled card before approving the transaction with a fingerprint scan or entering a PIN." See **Exhibit 14** (Samsung's Web Payments Integration Guide). A standard W3C implementation of Samsung Pay to a standard PaymentRequest object is shown below:



61. Samsung Pay also works with merchant apps on a user's smartphone. On information and belief, merchant apps installed on a user's smartphone communicate with Samsung Pay through the Samsung Pay API. A general use case takes the following form, according to Samsung:



62. To initiate payment, a merchant app calls the startIn-AppPay function of the API, which "initiates payment request with Samsung Pay." When the merchant app calls startIn-AppPay, Samsung Pay responds by presenting the user "with a payment sheet, which includes card selection and shipping address confirmation." After being presented the payment sheet, "the user then authenticates the payment method, amount, and delivery address with a fingerprint."

63. Samsung Pay also operates using NFC and/or MST: "Combining NFC with Samsung's proprietary MST technologies, Samsung Pay provides consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." *See* **Exhibit 15** (Samsung Pay Reaches One Year Anniversary in the United States, Samsung Newsroom (2016)). Samsung Pay equipped devices utilize the Android OS, as noted above. "Android 4.4 introduce[d] a new platform support for secure NFC-based transactions through Host Card Emulation (HCE), for

payments, loyalty programs, card access, transit passes, and other custom services." **Exhibit 16** (Android KitKat). When a user taps a phone to a payment terminal, "Android uses Application Identifiers (AIDs) as defined in ISO/IEC 7816-4 as the basis for routing transactions to the correct Android applications", such as the equipped Samsung Pay on Samsung's devices. When paying with Samsung Pay instore, "the app reads the transaction data and can use any local or network-based services to verify and then complete the transaction." *Id.* When opened in response to AID routing, Samsung Pay permits a user "to make a payment with [their] Favorite Cards, [by] swip[ing] up from the bottom of the screen. Then swip[ing] through and select[ing their] preferred card." *See* **Exhibit 17** (Make an in-store payment with Samsung Pay, Samsung Support). After selecting the card, the user "tap[s] PIN or IRIS . . . [or] simply place[s their] finger on [their] phone's fingerprint scanner". *Id.*.

64. Whether through AID routing, functions call between apps, or push notifications, regardless of where a user is shopping Samsung Pay equipped devices receive a request for biometric verification to authorize payment.

65. On Android devices like Samsung's devices, "the fingerprint sensor of [the] device is generally idle", but "in response to a call to authenticate . . . the fingerprint sensor listens for a touch". **Exhibit 18** (Android Open-Source Project: Fingerprint HIDL). After the user places their fingerprint on the sensor, a "vendor-specific library determines if there is a fingerprint match in the current set of enrolled fingerprint templates." *Id.*

66. Samsung Pay equipped devices wirelessly transmit EMV tokens to provide payment to merchants. When shopping online at a website, Samsung Pay equipped devices receive a push notification requesting authorization by the user, as detailed *supra*. "After user authenticates payment data is encrypted with partner's public key in user device, and will be sent

it to Samsung server" and made available to the merchant's website. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12.

67. The series of requests and responses permitting the merchant to receive payment, as summarized in Figure 10.1 of the EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020), begins with the merchant submitting a Token Payment Request for transaction routing. **Exhibit 20**. The data included within the Token Payment Request, as detailed in Table 10.1 of **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), is required to contain the payment token.

68. During transaction routing within the payment network, the Token Payment Request is transformed to a Token Authorization Request, as detailed in Figure 10.1 of **Exhibit 20**. As detailed in Table 10.3 of **Exhibit 20**, a required field of the Token Authorization Request generated by routing the Token Payment Request through payment network is a payment token. Accordingly, the payment token sent in the Token Payment Request from the merchant continues to persist during the token authorization request process. EMV payment tokens uniquely identifying Samsung Pay equipped devices and are provided during card enrollment, and thus are an identified embodiment of device ID codes specifically mentioned in at least the 730, 905, and 989 Patents.

69. "The Token Authorisation request process continues until De-Tokenisation has been completed." **Exhibit 20**, page 86. De-Tokenisation is performed by the token service provider. Visa, MasterCard, American Express and Discover each take on the role as TSPs. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers). "Token Service Providers are responsible for a number of discrete

functions which may include, but are not limited to: Maintenance and operation of a Token Vault . . . [and] De-Tokenisation". **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), page 19.

70. Maintaining the token vault and providing de-tokenisation, token service providers keep a list of device ID codes uniquely identifying legitimate integrated devices. The token vault maintained by Visa, MasterCard, and other token service providers is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data". Maintaining the mapping between payment tokens and underlying primary account numbers, the token vault represents a list of legitimate tokens. EMV payment tokens, as detailed above, are values uniquely identifying Samsung Pay-equipped devices provided during card enrollment, and thus are an identified embodiment of device ID codes. As tokens are embodiments of device ID codes, the listing of legitimate payment tokens maintained by token service providers as part of the token vault is an identified embodiment of a list of device ID codes uniquely identifying legitimate integrated devices. TSPs are therefore one embodiment of a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices.

71. Opening the token vault to perform de-tokenisation occurs in response to receiving the token authorization request containing the payment token. De-Tokenisation is "the process of converting a Payment Token and Token Expiry Date to its underlying PAN and PAN Expiry Date based on the Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date stored in the Token Vault." **Exhibit 20** at 6. "The Payment Token SHALL be de-tokenised to the underlying PAN in the incoming Token Authorisation prior to sending the PAN Authorisation to the Card Issuer." *Id.*, at 91. Detokenizing in response to an incoming token

authorization requests requires the token service provider be sent the token authorization. As noted above, the token authorization sent to the TSP contains the payment token wirelessly sent from a Samsung Pay-equipped smartphone after successful biometric authentication. Authenticating a user via biometrics, as noted above, entails a vendor-specific library on the Samsung Pay-equipped devices comparing scan data from a sensor to biometric data to determine whether the scan data matches the biometric data.

72. When providing payment for in-app purchases, Samsung Pay equipped devices wirelessly transmit EMV tokens to merchants as payment. Specifically, "Encrypted payment information is passed from the Samsung Pay to the PG [(Payment Gateway)] through the merchant app". **Exhibit 21** (Samsung Pay Developers Onboarding and Project Integration Guide: In-App Payments for Merchants, Doc Rev 3.1-US (2017)), page 17.

73. In addition to providing payment information via virtual terminals, Samsung Pay equipped devices "combin[e] NFC with Samsung's proprietary MST technologies [to provide] consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." Tapping a credit card is an example of contactless payment. "In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]) or NFC." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 39. By utilizing NFC, Samsung Pay-equipped devices can wirelessly transmit payment information to in-store terminals.

74. After the purchase has been authorized, Samsung Pay equipped devices "receive a push notification with details of [the] transaction after each purchase." **Exhibit 23** (View recent transactions in Samsung Pay). As the purchase can only be made after the primary account number

mapped to the token was released from the token vault and placed in an authorization request sent to the card issuer, the push notification received indicates allowed access to the file containing the account number. As shown in Figures 6, 7 and 11 of **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), this confirmation of access is either sent directly from the token service provider or indirectly from the token service provider as one of series messages flowing back to the Samsung Pay equipped smartphone.

75. Samsung Pay functionality is not limited to Samsung smartphone and tablet devices. Samsung's Galaxy Watch series also integrates with Samsung Pay. Samsung advertises that "you can use Samsung Pay on your watch!" An image that appears on Samsung's support page titled "Setting up your Samsung smart watch with or without your phone" is reproduced below:



76. The same support page describes that "[t]o access all its fun and useful features, you'll want to connect your smart watch to your phone using the Galaxy Wearable app.." **Exhibit 24**. As such, a Samsung smartphone or tablet with the Samsung Galaxy Wearable app (Wear

App) installed may act a personal digital key. Samsung smartphones and tablets communicate wirelessly, via an integrated receiver-decoder circuit enabling communication via Bluetooth, for example, with the Samsung Galaxy Watch, which also contains a receiver-decoder circuit external to the phone or tablet.

77. Samsung smartphone and tablets utilize a system on a chip (SoC) such as, in the case of its latest Galaxy S21 model, the Qualcomm Snapdragon 888 which provides several wireless interfaces including 5G, LTE, Bluetooth, and Wi-Fi. When communicating over a Bluetooth wireless connection, a proximity zone between the two devices is inherent, as the Bluetooth range may be approximately 30 feet.

78. The SoC interfaces with the various system components including the secure element, which is utilized to store, *inter alia*, secure biometric information for authenticating a user. The SoC must, like other system components, also interface with the battery of the smartphone or tablet.

79. On information and belief, Samsung's execution environment for Samsung Pay on its Galaxy Watch series includes an embedded secure element ("eSE"). Samsung has indicated such to EMVCo, as per the EMVCo Letter of Approval for the Galaxy Watch Active 2. eSE provides embedded, secure storage to "keep mobiles safe" by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." **Exhibit 25** (Samsung Security Solutions, Embedded security keeps mobiles safe).

80. The personal digital key component of Samsung's devices enable, *inter alia*, Samsung Pay.

81. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees have also complied with the marking provisions of 35 U.S.C. § 287.

CLAIM 1
(Infringement of the 730 Patent)

82. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

83. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 730 Patent.

84. Samsung infringes at least claims 1, 2, 5, 6, 8, and 9 of the 730 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

85. For example, Samsung directly infringes at least claim 1 and 5 of the 730 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States the software application Samsung Pay and products including Samsung Pay (*see* Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of the device.

86. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint and/or iris profile of a user, and codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value, in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered. Samsung devices utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example,

Samsung devices may utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

87. Samsung devices with Samsung Pay safeguard financial information, *e.g.*, credit card information, with EMV payment tokens as described *supra*. Indeed, Samsung was among the first to implement EMV payment tokens in digital wallets that hold credentials. On information and belief, the EMV payment tokens utilized by Samsung Pay uniquely identify the Samsung device. On further information and belief, the payment tokens are stored in a secure element that is tamper proof, *e.g.*, the Infineon SLE 97 ICC chip in the Galaxy S6 and S6 Edge. Secure elements are recognized as "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

88. Samsung devices with Samsung Pay also contain a secret decryption value, also called a "private key," which is used for, *inter alia*, decrypting, as specified in Android's keymaster functions, which provide hard-backed cryptography for secure key storage in a secure environment, such as the TEE, described *supra*. The secret decryption value, like the biometric data of the user and plurality of codes and other data values comprising a device idea, is tamper-proof as a result of being securely stored by the Samsung devices.

89. As described *supra*, Samsung devices with Samsung Pay may utilize biometric data, such as fingerprint and/or retina scan data from a biometric scan, and verify (*e.g.*, authenticate) biometric data of a user. The location of a purchase may determine how the request for verification is received (*e.g.*, a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores). When a Samsung device utilizes and verifies fingerprint biometric data,

for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

90. After receiving the determination that the scan data matches the biometric data, Samsung devices with Samsung Pay wirelessly send one or modes codes, including device ID codes, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens. EMV payment tokens, as detailed *supra*, are values uniquely identifying Samsung Pay preloaded smartphones provided during card enrollment, and thus are an identified embodiment of device ID codes. The payment tokens may be authenticated by an agent, *e.g.*, a token service provider.

91. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, e.g., token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token, which includes one or more codes from a plurality of codes and other data values including a device ID device, wirelessly transmitted by a Samsung device to the tokens stored in its repository for authenticated.

92. Samsung devices with Samsung Pay are further responsive to authentication by the agent, *e.g.*, token service providers, of the one or more codes and the other data values. For example, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. The push notification from the agent indicates that the user has been allowed access to an application, for example, an ATM machine, computer software, a web site and/or a file, *e.g.* which permits payment to occur.

93. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 730 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

94. Samsung also contributes to infringement by others of one or more claims of the 730 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 730 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

95. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 730 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 730 Patent.

96. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

97. Upon information and belief, Samsung will continue to infringe the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Samsung.

CLAIM 2
(Infringement of 905 Patent)

98. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

99. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 905 Patent.

100. Samsung infringes at least claims 1, 4, 5, 7, 9, 10, and 12 of the 905 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

101. For example, Samsung directly infringes at least claim 1 of the 905 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with Samsung Pay (see Appendix A). That software performs/executes, and those products provide, the method of claim 1, for example.

102. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or retina data, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

103. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (e.g., PAN) with another numeric value." *Id.*, at 8. Payment tokens, accordingly, are issued ("provisioned") to Samsung Pay preload smartphones in

exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id.*, at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

104. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and iris-scanning, to verify a user. The location of a purchase may determine how the request for verification is received (*e.g.*, a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores).

105. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26** (Samsung Pay Web checkout Integration guide, Document version 1.4 (2018)), page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id.*, at 6. Receiving a push notification prompting the user to authenticate by paying with their fingerprint, Samsung Pay preloaded smartphones therefore receive a request for biometric verification. Furthermore, Samsung devices with Samsung Pay receive scan data from a biometric scan carried out on a biometric sensor in response to receiving a request for biometric verification of a user.

106. When a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data from the fingerprint sensor of the device is compared with the existing fingerprint data on the device to determine whether there is a match.

107. After authenticating a user, Samsung devices with Samsung Pay wirelessly transmit one or modes codes, including device specific ID code, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

108. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, *e.g.*, token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

109. After an ID code has been authenticated by a third-party trusted authority, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. At this point, whereby the third-party trusted authority has confirmed that it successfully authenticated the token (*e.g.*, including the ID code), the user is allowed to complete a financial transaction.

110. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 905 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

111. Samsung also contributes to infringement by others of one or more claims of the 905 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly

infringe the 905 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

112. Samsung received actual and constructive notice of the 905 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 905 Patent.

113. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

114. Upon information and belief, Defendant will continue to infringe the 905 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 905 Patent by Defendant.

CLAIM 3
(Infringement of 989 Patent)

115. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

116. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 989 Patent.

117. Samsung infringes at least claims 1-6 of the 989 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

118. For example, Samsung directly infringes at least claim 1 of the 989 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with

Samsung Pay (see Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of a device.

119. As described *supra*, Samsung devices are approved by EMVCo. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19**(EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (*e.g.*, PAN) with another numeric value." *Id.*, p. 8. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. "[T]he TSP acts as a trusted service manager (TSM), delivering the token over the air or over an Internet connection to a device," *e.g.*, Samsung devices with Samsung Pay. *Id.*, p. 12. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. This token, received by the Samsung devices, therefore contains an ID code that uniquely identifies the smartphone among a plurality of smartphones.

120. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or iris profile of a user, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) which limits access to, and the ability to alter, biometric data.

121. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. Payment tokens are issued ("provisioned") to

Samsung devices with Samsung Pay in exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id.*, at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

122. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and retina data, and authenticate such biometric data. The location of the purchase determines the type of verification carried out (*e.g.*, a merchant's website, merchant apps installed on the device, or use of NFC (or MST) that provides a "way to pay almost anywhere you can swipe or tap a card at millions of merchant locations."

123. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26**, page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id.*, at 6. As part of the authentication, Samsung devices with Samsung Pay receive scan data from a biometric scan using the smartphone.

124. Where a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

125. After authenticating a user (*e.g.*, making a determination that the scan data matches the biometric data), a Samsung device with Samsung Pay wirelessly sends one or modes codes, including device specific ID code, regardless of where the user is shopping, to a third-party trusted authority, *e.g.*, token service providers. For example, Samsung devices wirelessly transmit EMV

payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

126. Token service providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

127. In response to a purchase having been authorized (e.g., after successful comparison of the token sent by the Samsung device to the token(s) stored in the repository) by the provider, the transaction is completed and the Samsung device "receive[s] a push notification with details of [the] transaction after each purchase." The transaction includes either access to an ATM machine or a financial account (e.g., a credit card).

128. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 989 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

129. Samsung also contributes to infringement by others of one or more claims of the 989 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 989 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

130. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 989 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement,

with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 989 Patent.

131. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 989 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

132. Upon information and belief, Defendant will continue to infringe the 989 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 989 Patent by Defendant.

CLAIM 4
(Infringement of 188 Patent)

133. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

134. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 188 Patent.

135. Samsung infringes at least claims 1, 3-10, and 13-16 of the 188 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

136. For example, Samsung directly infringes at least claims 1 and 10 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 10 and those products provide the hybrid device of claim 1, for example.

137. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured biometric information.

138. The key utilized by the Wear App to control access to the memory of the Android smartphone by a paired Galaxy Watch may take on various forms. The key may be a cryptographic key such that an "encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key)". 188 Patent, Col. 6, ll. 33-37. In lieu of cryptology, the key may uniquely identify the paired Galaxy Watch. In such instances, the key may be "a PDK ID 212 [] used as an identifying feature of a PDK 102 and distinguish[ing] between PDKs 102 in private or Central registry entries". *Id.*, Col. 5, ll. 66 to Col. 6, ll. 2. Besides a unique identifier or crypto-key, the key used by the Wear App to control memory access by a paired Galaxy Watch may be a "basic authentication function that allows the PDK and sensor to verify each other. In this scenario, once the sensor and PDK finish their verification the application is signaled". *Id.*, Col. 9, ll. 28-31 ("[T]he RDC 304a represents and includes the functionality described above as being provided by the sensor 108." Id, Col. 13, ll. 58-60.).

139. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access keys to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control

access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id.* By pairing a Galaxy Watch with the Samsung device, the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

140. Samsung devices, including those with the Samsung Galaxy Wearable app, store local, secured biometric information as per Android's implementation guidelines which require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". Exhibit R (Android Open-Source Project: Fingerprint HIDL). Per these guidelines, biometric information, *e.g.*, fingerprint data never leaves the TEE. Furthermore, Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted exaction environment" isolated from the rest of the system. **Exhibit 28** (Android Open-Source Project: Trusty TEE). Accordingly, biometric information, *e.g.*, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing, Trusty.

141. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, e.g. Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy

Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

142. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, inter alia, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—e.g., a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

143. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". Id. Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

144. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13,

EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Exhibit 25 (Embedded security keeps mobiles safe). Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

145. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

146. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, inter alia, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

147. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 188 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

148. Samsung also contributes to infringement by others of one or more claims of the 188 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

149. Samsung received actual and constructive notice of the 188 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 188 Patent.

150. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 188 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

151. Upon information and belief, Defendant will continue to infringe the 188 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

CLAIM 5
(Infringement of 700 Patent)

152. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

153. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 700 Patent.

154. Samsung infringes at least claims 1, 3, 5-9, 11, 15-17 and 19 of the 700 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

155. For example, Samsung directly infringes at least claims 1 and 11 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 11 and those products provide the hybrid device of claim 1, for example.

156. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured financial information.

157. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access secured financial information (*e.g.*, keys) to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id.* By pairing a Galaxy Watch with the Samsung device,

the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

158. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, *e.g.* Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

159. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, *inter alia*, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—*e.g.*, a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

160. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use

Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". *Id.* Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

161. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13, EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Embedded security keeps mobiles safe, http://www.samsung.com/semiconductor/security/ese/. Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

162. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to

transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

163. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, *inter alia*, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

164. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 700 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

165. Samsung also contributes to infringement by others of one or more claims of the 700 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

166. Samsung received constructive notice of the 700 Patent at least as early as July 2017 and actual notice of the 700 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 700 Patent.

167. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 700 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

168. Upon information and belief, Defendant will continue to infringe the 700 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants infringe one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendants' infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendants' infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: March 5, 2021

Respectfully submitted,

/s/ Erick S. Robinson

David L. Hecht (PHV to be submitted) (**lead counsel**)
Maxim Price (PHV to be submitted)
Conor B. McDonough (PHV to be submitted)
Yi Wen Wu (PHV to be submitted)
James Zak (PHV to be submitted)
dhecht@hechtpartners.com
mprice@hechtpartners.com
cmcdonough@hechtpartners.com
wwu@hechtpartners.com
jzak@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821
dhecht@hechtpartners.com

-and-

Erick S. Robinson
Texas Bar No. 24039142
erobinson@porterhedges.com
PORTER HEDGES LLP
1000 Main Street, 36th Floor
Houston, Texas 77002
P (713) 226-6615
F: (713) 226-6215

ATTORNEYS FOR PLAINTIFF
Proxense, LLC

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

PROXENSE, LLC, Plaintiff, v. SAMSUNG ELECTRONICS CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC. Defendants.	Civil Action No.: 6:21-cv-00210-ADA **JURY TRIAL DEMANDED** **ORAL ARGUMENT REQUESTED**

DEFENDANTS' OPPOSED MOTION
FOR LEAVE TO AMEND INVALIDITY CONTENTIONS

TABLE OF CONTENTS

Page

I. BACKGROUND 2
A. Samsung Timely Served Its Amended Invalidity Contentions for the Pocket Vault System. 2
B. New References Introduced In Light Of PTAB Denied Institution of IPRs. 3
II. LEGAL STANDARD 6
III. GOOD CAUSE EXISTS FOR SAMSUNG'S SUPPLEMENTATION OF POCKET VAULT SYSTEM ART OBTAINED DURING DISCOVERY 6
A. The Factor 1 – Samsung Has Been Diligent in Locating Additional Evidence to Support Their Invalidity Theories with Respect to Pocket Vault 6
B. Factor 2 – Pocket Vault is Important Prior Art and Invalidating the Patents in Suit Would be Case Dispositive 8
C. Factor 3 – Proxense Will Suffer No Prejudice 9
D. Factor 4 – A Continuance is Unnecessary for the Amendments 11
IV. GOOD CAUSE EXISTS FOR SAMSUNG'S SUPPLEMENTAL REFERENCES LOCATED FOLLOWING THE PTAB'S DECISION 11
A. Factor 1 - Samsung Diligently Searched for Supplemental Art 11
B. Factor 2 - The Proposed Amendments are Important Prior Art and Invalidating the Patents in Suit Would be Case Dispositive 14
C. Factor 3 - Proxense Does Not, and Cannot Argue Prejudice 14
D. Factor 4 - A Continuance is Unnecessary for the Amendments 15
V. CONCLUSION 15

TABLE OF AUTHORITIES

Page

Cases

Allure Energy, Inc. v. Nest Labs, Inc.,
84 F. Supp. 3d 538 (E.D. Tex. 2015) 12, 14

Apple Inc. v. Samsung Elecs. Co.,
No. 12-CV-0630-LHK PSG, 2013 WL 3246094 (N.D. Cal. June 26, 2013) 12

CellCast Techs., LLC v. United States,
152 Fed. Cl. 414 (2021) 13

Estech Sys., Inc. v. Target Corp.,
No. 2:20-cv-00123-JRG-RSP, 2021 WL 2187978 (E.D. Tex. May 28, 2021) 9, 14

Garrity Power Servs. LLC v. Samsung Elecs. Co.,
No. 2:20-CV-00269-JRG, 2021 WL 4894262 (E.D. Tex. Oct. 19, 2021) 8

GPNE Corp. v. Apple Inc.,
No: 5:12–cv–02885–LHK, 2013 WL 6157930 (N.D. Cal. Nov. 22, 2013) 13

Hearing Components, Inc. v. Shure, Inc.,
No. 9:07CV104, 2008 WL 11348009 (E.D. Tex. June 5, 2008) 11

Kinglite Holdings Inc. v. Micro-Star Int'l Co.,
No. CV1403009JVSPJWX, 2015 WL 6437836 (C.D. Cal. Oct. 16, 2015) 13

Kroy IP Holdings, LLC v. AutoZone, Inc.,
No. 2:13-cv-888, 2014 WL 7463099 (E.D. Tex. Dec. 30, 2014) 8

Maxell Ltd. v. Apple Inc.,
2020 WL 10456917 (E.D. Tex. Feb. 24, 2020) 13

Maxell Ltd. v. Apple Inc.,
No. 5:19-CV-00036-RWS, 2020 WL 10456917 (E.D. Tex. Feb. 24, 2020) 12

Mears Techs., Inc. v. Finisar Corp.,
No. 2:13-cv-376-JRG, 2014 WL 12605571 (E.D. Tex. Oct. 6, 2014) 8

MV3 Partners LLC v. Roku, Inc.,
No. 6:18-CV-00308-ADA (W.D. Tex. Mar. 23, 2020) 6

O2 Micro Int'l Ltd. v. Monolithic Power Sys., Inc.,
467 F.3d 1355 (Fed. Cir. 2006) 6

Regents of Univ. of California v. Affymetrix, Inc.,
No. 17-CV-01394-H-NLS, 2018 WL 4053318 (S.D. Cal. Aug. 24, 2018) 11

S&W Enterprises, L.L.C. v. SouthTrust Bank of Alabama, NA,
315 F.3d 533 (5th Cir. 2003) 6

TurboChef Techs., Inc. v. Garland Com. Indus., LLC,
No. 07-CV-1330-F, 2010 WL 11618339 (W.D. Tex. June 24, 2010) 13

Tyco Healthcare Grp. LP v. E-Z-EM, Inc.,
No. 2:07-CV-262 TJW, 2010 WL 7853420 (E.D. Tex. Apr. 1, 2010) 13

Uniloc 2017 LLC v. Google LLC,
No. 2:18-cv-00493-JRG, 2019 WL 6465318 (E.D. Tex. Dec. 2, 2019) 14

United Servs. Auto. Ass'n v. Wells Fargo Bank, N.A.,
No. 2:18-CV-00366-JRG-RSP, 2019 WL 6878880 (E.D. Tex. Dec. 17, 2019) 11

Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively "Samsung") seek leave to amend their invalidity contentions for good cause.

This is Samsung's first request to amend its invalidity contentions, and all of the information sought to be added was discovered after the deadline for final invalidity contentions. The proposed amendments fall into two general categories.

First, Samsung seeks leave to supplement preexisting invalidity charts regarding a prior art system (Pocket Vault) to add additional evidence that Samsung recently received from third parties with knowledge of the Pocket Vault system. Samsung received the additional evidence in mid-May; analyzed it and informed Proxense in late June of its intention to amend its contentions; and provided Proxense with a complete copy of its proposed amendments by July 8. *See* Williams Declaration, ¶ 2, Exs. A, I. The relevant third parties—three former employees of the company that developed Pocket Vault—were all deposed by the parties over the past week, such that Proxense has had a full opportunity during discovery to explore the evidence and Samsung's arguments. *See id.*, ¶ 6.

Second, Samsung seeks leave to add three new prior art references that Samsung discovered following the PTAB's decisions to deny institution of Samsung's petitions for *inter partes* review for the patents-in-suit. The PTAB's institution decisions were based on claim construction arguments Proxense did not advance in this Court. Following the institution decisions, Samsung diligently searched for this art, which is highly material to the validity of Proxense's patents. And following discovery of this art, Samsung concurrently analyzed the prior art and prepared petitions for *ex parte* reexamination ("EPR") of the three remaining patents-in-suit, serving the filed petitions (which include the extensive analysis performed by Samsung) on Proxense the same day the EPRs were filed. *See* Ex G. Samsung then provided a complete set of its proposed amended invalidity charts to Proxense on July 8, 2022. *See* Exs. B, I.

Good cause exists for Samsung to amend its final invalidity contentions because it was diligent in discovering the additional evidence, analyzing and disclosing it, and in seeking to amend. Further, Samsung believes the prior art Pocket Vault system and the new references that became relevant in light of the PTAB ruling are important evidence supporting Samsung's previously disclosed invalidity positions. Nor will Plaintiff suffer any unfair prejudice as a result of the amendments, as Plaintiff was put on notice of these proposed amendments several weeks before the close of fact discovery, and well before the depositions of the relevant witnesses. Furthermore, because these charts pertain to invalidity, an issue on which Samsung bears the burden, Plaintiff will not have to respond until rebuttal expert reports due in September 2022.

For all of these reasons, Samsung respectfully requests that this Motion be granted.

I. BACKGROUND

A. Samsung Timely Served Its Amended Invalidity Contentions for the Pocket Vault System.

On August 26, 2021, Samsung timely served its invalidity contentions for U.S. Patent Nos. 8,352,730 (the '730 patent), 9,298,905 (the '905 patent), and 10,698,989 Patent (the '989 Patent) (collectively the "Asserted Patents").[1] As part of preparing these invalidity contentions, Samsung located and charted relevant prior art, including the Pocket Vault system prior art and U.S. Patent Application Publication No. 2003/0220876 ("Burger") illustrating the embodiments of the Pocket Vault system. Samsung drafted invalidity charts, asserting that the Pocket Vault system and Burger anticipate and render obvious the asserted claims of the Asserted Patents. In both the invalidity charts addressing the Pocket Vault system and Burger, Samsung explicitly reserved the right to supplement the charts after additional discovery. The same charts were also included as

[1] Samsung's preliminary infringement contentions also covered patents no longer asserted in this action. Dkt. 62.

part of the final invalidity contentions served on March 7, 2022. These charts were based on publicly available materials describing the Pocket Vault system.

During fact discovery, Samsung pursued additional documents and materials regarding the Pocket Vault system, but did not begin receiving access to additional Pocket Vault materials until mid-May in 2022. *See* Williams Declaration, ¶ 2. In June, after analyzing the contents of the Pocket Vault production and deciding to amend its invalidity contentions, Samsung immediately asked if Proxense would consent to Samsung's amending its invalidity contentions. *See* Ex. C. In early July, Samsung sent Proxense a draft of its proposed amended invalidity charts for the Pocket Vault system—adding citations to documents that were newly received from Pocket Vault. *See* Exs. A, I. Samsung also met and conferred with Proxense regarding its motion for leave to amend invalidity contentions, but Proxense stated it would oppose Samsung's motion. *See* Williams Declaration, ¶ 5.

In mid-July, Samsung also served subpoenas on three Pocket Vault inventors – Stuart Lipoff, Todd Burger, and Brad Friedlander seeking their depositions. *See* Ex. D. Proxense did not respond. Approximately a week later, Samsung served deposition notices for the same three Pocket Vault inventors. In response, Proxense did not claim prejudice, but instead served its own deposition notices. The parties deposed the three inventors in the last week of July and the first week of August 2022, right before close of the fact discovery on August 8, 2022. *See* Williams Declaration, ¶ 6. Both parties had the opportunity to, and did, ask questions of all three Pocket Vault witnesses.

B. <u>New References Introduced In Light Of PTAB Denied Institution of IPRs.</u>

On August 26, 2021, the same day Samsung served its preliminary invalidity contentions, Samsung also filed *inter partes review* petitions ("IPRs") against each of the Asserted Patents. *See* IPR2021-01444 (PTAB Aug. 26. 2021) ("'730 Patent IPR"); IPR2021-01447 (PTAB Aug. 26.

2021) ("'905 Patent IPR"); IPR2021-01448 (PTAB Aug. 26. 2021) ("'989 Patent IPR"). In each of the three petitions, Samsung argued that "the claim terms should be given their plain and ordinary meaning." *See* '730 Patent IPR at 8, '905 Patent IPR at 7, '989 Patent IPR at 7-8. Samsung also noted that it "reserve[d] the right to pursue different claim constructions . . . during this and related proceedings." *Id.*[2]

On February 28, 2022, the PTAB denied institution of all three IPRs. *See* IPR2021-01444, Paper 11 (PTAB Feb. 28, 2022) ; IPR2021-01447, Paper 12 (PTAB Feb. 28, 2022) ; IPR2021-01448, Paper 11 (PTAB Feb. 28, 2022). The PTAB determined that Samsung had not shown a reasonable likelihood that it would prevail with respect to at least one of the challenged claims based on a claim construction position advocated by Proxense in its Preliminary Response. *See, e.g.,* IPR2021-01444, Paper 11 at 9, 12 (PTAB Feb. 28, 2022). Specifically, Proxense offered, and the PTAB construed "third-party trusted authority" "to mean a trusted authority that is an entity separate from the parties to a transaction." *Id.* at 15. The PTAB then determined that the prior art references which Samsung presented in the IPRs did not teach this construction for "third-party trusted authority." *Id.* at 27-28. For instance, the PTAB stated that one of the prior art references advocated by Samsung that it is not a "third-party trusted authority" because it is "not an entity separate [from itself]" and thus does not meet the claim limitation. *Id.* at 25.

Contrary to the construction Proxense offered during the IPR, in this litigation, Proxense offered the construction "[a] third component that provides a second level of authentication" as its proposed construction for "third-party trusted authority." Ex. F at 5. This construction did not include the "separate entity" language Proxense offered during the IPR and adopted by the PTAB.

[2] Additionally, for the '730 IPR, Samsung argued that "tamper proof format" applies to each of (1) "biometric data of the user," (2) "a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device," and (3) "a secret decryption value." '730 Patent IPR at 8-9.

Accordingly, Samsung addressed Proxense's district court construction in its opening claim construction brief. Dkt. 33 at 6. In its opposition brief, Proxense stated that it "no longer seeks to submit this term for construction." Dkt. 35 at 15. This term was subsequently never construed by this Court. *See generally* Dkt. 43. The PTAB's adoption of the construction was thus a new development that led Samsung to conduct additional prior art searches.

Samsung promptly began supplemental prior art searches in response to the IPR decisions, focusing on locating prior art that addressed the new and narrower construction adopted by PTAB. It timely served final infringement contentions on March 7, 2022. But it continued searching for any references which meet the "third-party trusted authority" limitation as construed by the PTAB, finding the art that is the subject of this motion after that deadline.[3]

Once Samsung found this new prior art, Samsung conducted the necessary analysis, simultaneously drafting EPRs. As soon as the analysis was complete, Samsung promptly filed the EPRs on June 8, 2022 based on the supplemental prior art it located in response to the PTAB's claim constructions: US Patent No. 7,188,110 ("Ludtke") and US Patent Publication No. 2003/0196084 ("Okereke").[4] Samsung served the EPRs via email on counsel of record in the litigation on June 8, 2022, more than two months prior to the close of fact discovery. Ex. G.

Shortly thereafter, on June 30, 2022, Samsung gave Proxense notice that "intends to supplement its invalidity contentions" in this action. Ex. C. Then, in early July, Samsung provided Proxense with fully fleshed-out claim charts for the three new references. Exs. B, I.

On August 1, 2022, the USPTO granted EPRs of all asserted claims of the Asserted Patents. *See* EPR 90/015,052 (PTAB June 8, 2022); EPR 90/015,053 (PTAB June 8, 2022); 90/015,054

[3] Samsung's final infringement contentions also stated that Samsung "reserves the right to supplement as further prior art is identified through investigation or discovery." Ex. H at 6.

[4] Although not part of the EPRs, the supplemental search also uncovered U.S. Patent No. 7,849,020 ("Johnson") which is also subject to this motion to supplement contentions.

(PTAB June 8, 2022). In granting EPRs, the USPTO concluded the Ludtke and Okereke references disclose technological teachings "that are deemed important to a reasonable examiner in determining the patentability of the claim 1 [of the '730 Patent]." *See, e.g.*, EPR 90/015,052 at 9. The USPTO found substantial new question of patentability on every ground raised by Samsung. *Id.*, at 10-12. Samsung will serve its invalidity expert report on August 15, 2022. Dkt. 48. Proxense's rebuttal validity report is not due until September 12, 2022. *Id.*

II. LEGAL STANDARD

A party may amend or supplement its invalidity contentions upon a showing of good cause. "'[G]ood cause' requires a showing of diligence." *O2 Micro Int'l Ltd. v. Monolithic Power Sys., Inc.*, 467 F.3d 1355, 1366 (Fed. Cir. 2006)). While courts have broad discretion to allow modifications, past decisions have considered the following four factors in ruling on such motions: (1) the explanation for the failure to meet the deadline; (2) the importance of the thing that would be excluded; (3) potential prejudice in allowing the thing that would be excluded; and (4) the availability of a continuance to cure such prejudice. *S&W Enterprises, L.L.C. v. SouthTrust Bank of Alabama, NA*, 315 F.3d 533, 535–36 (5th Cir. 2003); *see also MV3 Partners LLC v. Roku, Inc.*, No. 6:18-CV-00308-ADA, Dkt. 164 at *1-2 (W.D. Tex. Mar. 23, 2020) (granting leave to amend contentions).

All these factors weigh in favor of granting Samsung leave to supplement its invalidity contentions.

III. GOOD CAUSE EXISTS FOR SAMSUNG'S SUPPLEMENTATION OF POCKET VAULT SYSTEM ART OBTAINED DURING DISCOVERY

A. <u>The Factor 1 – Samsung Has Been Diligent in Locating Additional Evidence to Support Their Invalidity Theories with Respect to Pocket Vault</u>

Samsung has been diligent and pursued third party discovery throughout the discovery period. The only reason the citations to the additional Pocket Vault materials were not already

included in the preliminary and final invalidity contentions is that Samsung did not previously have access to these materials in this case.[5] The Pocket Vault witnesses began to provide materials regarding Pocket Vault to Samsung in mid-May. *See* Williams Declaration, ¶ 2. Samsung immediately began reviewing the materials to locate relevant portions to include in the invalidity contentions. By the end of June, Samsung had informed Proxense of its intention to amend its invalidity contentions to add citations to additional Pocket Vault evidence. Ex. C. About a week later, on July 8, Samsung also provided Proxense with the specific amended invalidity contention charts that are the subject of this motion. *See* Exs A, I. At the same time, Samsung also served subpoenas seeking the depositions of the Pocket Vault witnesses. *See* Ex. D. Samsung followed up with deposition notices, and Proxense also served deposition notices on the Pocket Vault witnesses. The depositions of the Pocket Vault witnesses took place at the end of July and the beginning of August. *See* Williams Declaration, ¶ 6.

The Pocket Vault materials date back 17 to 23 years and are not readily available. Courts have recognized that obtaining evidence from a defunct third-party company does not constitute delay, and have allowed supplementation in such circumstances. *See, e.g.*, *Garrity Power Servs. LLC v. Samsung Elecs.* Co., No. 2:20-CV-00269-JRG, 2021 WL 4894262, at *2-3 (E.D. Tex. Oct.

[5] All of the ten additional Pocket Vault documents added by Samsung to its amended Pocket Vault invalidity contention charts were not publicly available. *See* Ex. A at 92-93 (The additional Pocket Vault evidences are: PV Service Definition v0_12 ("Service Definition") (SAMSUNG_Proxense_208262); Provisioning Overview ("Overview") (SAMSUNG_Proxense_208713); Marzen Team Pro…11 Mar 2002 copy ("Marzen") (SAMSUNG_Proxense_208534); pocket vault spec_tob copy.doc ("Spec Tob") (SAMSUNG_Proxense_208697); TFarb VC CNI 101404 copy ("TFarb") (SAMSUNG_Proxense_209019); sec3.ppt ("Sec3") (SAMSUNG_Proxense_208344); CitiCNI mtg 120601 Q&A ("CitiCNI") (SAMSUNG_Proxense_208789); Visa Intl Tech Mtg 1204 v3 ("Visa Intl") (SAMSUNG_Proxense_209047); Brookstone FAQ v4 ("Brookstone") (SAMSUNG_Proxense_208729); and CNIFullBizPln-v11Flaster copy ("CNIFullBizPln") (SAMSUNG_Proxense_208141)). Samsung could not possibly include these additional evidences in its preliminary and final invalidity contentions—before receiving them from the Pocket Vault witnesses.

19, 2021) (granting a motion leave to amend invalidity contentions where the motion filed one day before the close of fact discovery. The amended contention contains information about a system art newly located by third-party discovery and plaintiff was put on notice of the existence of the prior art by preliminary contentions); *see also Kroy IP Holdings, LLC v. AutoZone, Inc.*, No. 2:13-cv-888, 2014 WL 7463099, at *2-3 (E.D. Tex. Dec. 30, 2014) (finding good cause to supplement invalidity contentions even though defendants first learned of the new prior art more than three months after the due date for filing invalidity contentions).

Proxense's only stated objection to this motion is premised on the timing of this motion. However, that objection ignores that the new Pocket Vault evidence was recently obtained and the motion merely seeks supplementing charts that has been in the case almost for a year. Furthermore, Proxense does not credibly refute Samsung's diligence. Proxense's reliance on *Mears Techs., Inc. v. Finisar Corp.*, No. 2:13-cv-376-JRG, 2014 WL 12605571, at *2 (E.D. Tex. Oct. 6, 2014) is flawed. In *Mears*, plaintiff sought to amend its infringement contentions twice: once to add additional products, and then to change its theory. Importantly, the court did allow the moving party to supplement based on information that was "recently learned," as is the case here. *Id.* at *1-2. As for the denial, plaintiff's request was a change its theory, came after the close of fact discovery, and on the eve of trial. No such facts exist here.

In this case, the record shows that Samsung has exercised diligence in seeking to amend its invalidity contentions based on recently produced third party documents.

B. Factor 2 – Pocket Vault is Important Prior Art and Invalidating the Patents in Suit Would be Case Dispositive

Samsung believes the Pocket Vault system invalidates the Asserted Patents and therefore the amendment of the invalidity contentions is important. Samsung expects to rely on the Pocket Vault system art as part of its case at trial. The documents and exhibits describing the Pocket Vault system art will be important to help show the jury how the Pocket Vault system invalidates the

alleged inventions of the Asserted Patents. Specifically, the recently produced documents cited in the amended invalidity contentions will provide jurors a visual representation of the Pocket Vault system, including the steps of the claimed user authentication process, which will help the trier-of-fact understand how the product invalidates the alleged invention. Thus, any amendment that would be dispositive of Proxense's claims is important and weighs in favor of granting Samsung's motion. *Estech Sys., Inc. v. Target Corp.*, No. 2:20-cv-00123-JRG-RSP, 2021 WL 2187978, *4 (E.D. Tex. May 28, 2021) (references are important for purposes of amending invalidity contentions because "[i]f Defendant's theory is accepted, patents-in-suit may be invalid").

Proxense's assertion that Samsung needs to show that Chameleon Networks has "reduce[d] [its] conceived invention to practice" is misplaced because it is not an issue to be decided at this stage. It appears that Proxense disputes Samsung's contention that the evidence cited in the amended invalidity contentions, as well as the Pocket Vault witnesses' testimony, demonstrates that Pocket Vault system was conceived, reduced to practice and offered for sale prior to the priority date of the Asserted Patents. But this dispute should not be resolved at this stage, and the present motion simply presents the threshold issue whether Samsung's should be granted leave to amend its invalidity contentions, which is decided based on factors such as timeliness, diligence and lack of prejudice. Proxense's issue will be resolved after the evidence for the invalidity theory is presented and vetted through expert reports, expert testimony, as well as later briefing and consideration by the jury.

C. Factor 3 – Proxense Will Suffer No Prejudice

Samsung has asserted the Pocket Vault system as prior art as early as the Preliminary Invalidity Contentions, served in August 2021, including both a chart on the Pocket Vault system as well as a chart on the Burger patent application. Therefore, Proxense has been on notice of

Samsung's invalidity theory for almost a year and has had the opportunity to pursue discovery into the Pocket Vault system during that entire time.

Samsung informed Proxense of its intent to amend its invalidity contentions on June 30, over a month before the close of fact discovery. Samsung provided its amended invalidity contentions to Proxense on July 8, a full month before the close of fact discovery. During this time, Proxense had the opportunity to, and actually did, pursue discovery into Pocket Vault. When Samsung sent deposition notices to Proxense informing Proxense of the time and place that Pocket Vault witnesses would be deposed, Proxense responded with deposition notices of its own and sent an attorney to each of the depositions, who asked questions of the Pocket Vault witnesses at each deposition. Indeed, some of the questions asked by Proxense during deposition related directly to the documents Samsung added in its amended invalidity contentions. *See* Ex. L at 175:3-179:2 (Proxense asked question specifically directed towards Exhibit 21 (SAMSUNG_Proxense_208789) and Exhibit 10 (SAMSUNG_Proxense_209047)—both of which are cited as additional Pocket Vault documents in Samsung's amended invalidity contentions charts). Thus, Proxense has had full opportunity to conduct discovery into Pocket Vault and to explore any issue it wished regarding Samsung's amended contentions.

Furthermore, on the issue of invalidity, Samsung as the defendant bears the burden of proof, and thus Proxense does not need to serve its expert report on validity until September 12, during rebuttal expert reports. Proxense thus has almost an entire month more than Samsung to analyze the Pocket Vault evidence. Proxense will further have the opportunity to depose Samsung's expert regarding the evidence contained within Samsung's amendment. *United Servs. Auto. Ass'n v. Wells Fargo Bank, N.A.*, No. 2:18-CV-00366-JRG-RSP, 2019 WL 6878880, at *2 (E.D. Tex. Dec. 17, 2019) (prejudice factor weighs in favor of finding a good cause because expert depositions have not yet occurred so there will be a full and fair opportunity to question the experts

regarding the amendment). Proxense did not claim it suffered any prejudice during the meet and confer and objected only on the basis of timeliness.

D. Factor 4 – A Continuance is Unnecessary for the Amendments

The addition of the additional Pocket Vault evidence will not require any change in the case schedule. *Regents of Univ. of California v. Affymetrix, Inc.*, No. 17-CV-01394-H-NLS, 2018 WL 4053318, at *4 (S.D. Cal. Aug. 24, 2018) (finding good cause to amend where "Defendants' proposed amended invalidity contentions would not pose a risk to any of the above discovery and motion deadlines or the Court's trial schedule."). As noted above, under the existing court schedule, Proxense has already had the opportunity to depose the Pocket Vault witnesses, and will have the benefit of deposing Samsung's expert on the Pocket Vault invalidity positions. Under the existing schedule, Proxense will have until September 12, 2022 to prepare its rebuttal expert report on validity. None of these timelines necessitates a continuance.

IV. GOOD CAUSE EXISTS FOR SAMSUNG'S SUPPLEMENTAL REFERENCES LOCATED FOLLOWING THE PTAB'S DECISION

A. Factor 1 - Samsung Diligently Searched for Supplemental Art

Once Samsung received the IPR denials, Samsung promptly began searching for supplemental prior art that met the limitations of the Asserted Patents using this construction. The process of finding and analyzing art is time consuming. *Hearing Components, Inc. v. Shure, Inc.*, No. 9:07CV104, 2008 WL 11348009, at *2 (E.D. Tex. June 5, 2008) (finding three-month delay "can be expected when a party conducts a proper investigation into the merits of its potential defenses"); *see also Maxell Ltd. v. Apple Inc.*, No. 5:19-CV-00036-RWS, 2020 WL 10456917, at *2 (E.D. Tex. Feb. 24, 2020). The fact that Samsung was not able to locate and chart new and different prior art by the final infringement deadline of March 7, 2022 – ***one week from when it received the IPR decisions*** – does not mean that Samsung failed to exercise diligence in this case, as Proxense has suggested. In fact, the default rules of this Court give a defendant ***eight weeks*** to

serve Final Infringement and Invalidity Contentions after fact discovery opens. *See* Standing Order Governing Proceedings (OGP) 4.1 – Patent Cases ("OGP") at 13. Moreover, the OGP explicitly says that the Final Invalidity Contentions "deadline ***does not relieve the parties of their obligation to seasonably amend if new information is identified after initial contentions***." *Id.* (emphasis added). That is precisely what Samsung did.

With respect to any delay, Proxense only relies on jurisprudence from another district's particular procedural rules (E.D. Tex.)—*Imperium IP Holdings (Cayman), Ltd. v. Samsung Elecs. Co.*, No. 4:14-CV-371, 2016 WL 3854700, at *2 (E.D. Tex. Mar. 28, 2016) and *Allure Energy, Inc. v. Nest Labs, Inc.*, 84 F. Supp. 3d 538, 542 (E.D. Tex. 2015). In the Eastern District of Texas, claim construction briefing takes place ***after*** invalidity contentions are served, and ***after*** discovery starts, and amended invalidity contentions can be served without a showing of good cause ***only if*** a party claiming patent infringement has served amended infringement contentions or "the party opposing a claim of patent infringement believes in good faith that the Court's Claim Construction Ruling so requires." E.D. Tex. Patent L. R. 3-6. By contrast, under the OGP of this Court, final invalidity contentions are mandatory ***after*** the Markman hearing. *See* OGP at 13. Unlike the other factors, delay should be considered based on the particular patent rules of the specific jurisdiction. It does not make sense that delay and diligence under a different governing claim construction, discovery, and docket control schedule should apply in this Court. Indeed, cases from this District have found granted amendments of invalidity contentions ***after*** service of opening and rebuttal expert reports and filing of summary judgment briefs. *See TurboChef Techs., Inc. v. Garland Com. Indus., LLC*, No. 07-CV-1330-F, 2010 WL 11618339, at *2 (W.D. Tex. June 24, 2010).

To the extent cases from other jurisdictions should be considered for this factor, courts have found that parties have acted diligently in supplementing their invalidity contentions under analogous situations. In this case, based on PTAB's construction, Samsung promptly found and

analyzed additional art, promptly filed EPRs after the analysis was complete and concurrently disclosed the analysis to Proxense, and then followed up with complete claim charts; all before close of fact discovery. *See Maxell.*, 2020 WL 10456917, at *2 (delay in discovering new reference is excusable where "litigation counsel, an additional intellectual property law firm and a prior art search firm all conducted extensive prior art searches"); *Tyco Healthcare Grp. LP v. E-Z-EM, Inc.*, No. 2:07-CV-262 TJW, 2010 WL 7853420, at *1 (E.D. Tex. Apr. 1, 2010) (granting leave to supplement invalidity contentions sought six months before trial); *accord GPNE Corp. v. Apple Inc.*, No: 5:12–cv–02885–LHK, 2013 WL 6157930, at *2 (N.D. Cal. Nov. 22, 2013) ("GPNE could not have anticipated the full scope of the amendments needed without the court's claims construction order before it."); *Kinglite Holdings Inc. v. Micro-Star Int'l Co.*, No. CV1403009JVSPJWX, 2015 WL 6437836, at *3 (C.D. Cal. Oct. 16, 2015) ("Kinglite still establishes its diligence in trying to amend its infringement contentions after the Court's Claim Construction Order. The Court's adoption of differing constructions from those proposed by Kinglite gives rise to good cause because those differences are material to Kinglite's theory of infringement."); *Apple Inc. v. Samsung Elecs. Co.*, No. 12-CV-0630-LHK PSG, 2013 WL 3246094, at *9 (N.D. Cal. June 26, 2013) ("[T]he court finds that the claim construction order provides good cause for the proposed amendments…"); *CellCast Techs., LLC v. United States*, 152 Fed. Cl. 414, 426 (2021) (agreeing that "the Claim Construction Order triggered the new search for prior art by the Defendants").

Samsung acted diligently in locating new art and Proxense has been on notice of the additional art since at least June 8, 2022 (in the case of the Ludtke and Okereke references) and July 8, 2022 (in the case of the Johnson reference). *See* Exs. G, I . Samsung's amendment will not impact the procedural schedule.

B. Factor 2 - The Proposed Amendments are Important Prior Art and Invalidating the Patents in Suit Would be Case Dispositive

Samsung's amendments are important and not cumulative. The references were first discovered in response to a claim construction argument not advanced in this Court and thus not cumulative. These references are important: when instituting EPRs for the Asserted Patents based on two of these references, the USPTO expressly identified the references as important in determining the patentability of the asserted claims. *See* EPR 90/015,052, Order Granting Request for *Ex Parte* Reexamination at 9 (PTAB August 2, 2022); EPR 90/015,053 Order Granting Request for *Ex Parte* Reexamination at 9 (PTAB August 2, 2022); EPR 90/015,054 Order Granting Request for *Ex Parte* Reexamination at 21 (PTAB August 2, 2022). This factor weighs in favor of granting the motion to amend. *Uniloc 2017 LLC v. Google LLC*, No. 2:18-cv-00493-JRG, 2019 WL 6465318, at *2 (E.D. Tex. Dec. 2, 2019) ("Prior art references potentially rendering a patent invalid are important."); *see also Estech Sys., Inc. v. Target Corp.*, No. 2:20-cv-00123-JRG, 2021 WL 2187978, *4 (E.D. Tex. May 28, 2021). According to the most recent EPR data from the Patent Office, the majority of granted EPR requests – almost 80% – result in the claims either being canceled or amended. *See* Ex. J.

C. Factor 3 - Proxense Does Not, and Cannot Argue Prejudice

Proxense will not be prejudiced by the inclusion of these few additional references. Indeed, the only argument which Proxense made in its original dispute chart based on prejudice was merely the fact that Samsung seeks to supplement its invalidity contentions "after parties have disclosed and argued for their claim construction positions." *See* Ex. E (citing *Imperium*, 2016 WL 3854700, at *2; *Allure Energy*, 84 F. Supp. 3d at 542). This argument is misplaced, since Proxense does not rely on cases for this District and Court, where final infringement contentions are due ***by default*** after claim construction positions are argued. *See* OGP at 13. Proxense thus has no credible prejudice arguments. Indeed, if Proxense's argument amounted to prejudice, then any final

contentions served in accordance with the procedural schedule in any case in this Court would by default prejudice the party receiving the supplement.[6]

Additionally, Samsung disclosed full analyses via the EPRs on June 8, 2022, and also provided Proxense with its proposed amended contentions on July 8, 2022, for purpose of mitigating any putative prejudice. Moreover, the close of expert discovery is still months away and Samsung has not yet served its opening invalidity expert report. If Samsung has enough time to prepare an opening report on invalidity on the supplemental references, then Proxense has more than enough time to write the rebuttal expert report. There is no prejudice to which Proxense can point based on the facts and schedule.

D. Factor 4 - A Continuance is Unnecessary for the Amendments

For the same reason as those in Section III.D, a continuance is not necessary.

V. CONCLUSION

Samsung respectfully requests that the Court grants Samsung's motion to amend its final invalidity contentions as to Pocket Vault system as set forth in Exhibit A. Samsung also seeks to amend its invalidity contentions as to the new references as Exhibit B.

[6] Proxense is further not prejudiced by the supplement because it was *Proxense's offered construction* in the IPRs that led to the supplement. Proxense chose to offer competing constructions in this litigation and the IPR, and, as the offeree, was aware of both of these constructions.

Dated: August 5, 2022

/s/ Victoria F. Maroulis
Kevin P.B. Johnson
kevinjohnson@quinnemanuel.com
Victoria F. Maroulis
victoriamaroulis@quinnemanuel.com
Mark Tung
marktung@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

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

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

Scott L. Cole
scottcole@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan, LLP
201 West 5th Street
11th Floor
Austin, TX 78701
Telephone: (737) 667-6104

Counsel for Defendants Samsung Electronics, Co., Ltd. and Samsung Electronics America, Inc.

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on August 5, 2022, all counsel of record who have appeared in this case are being served with a copy of the foregoing via the Court's CM/ECF system.

Dated: August 5, 2022

/s/ Victoria F. Maroulis
Victoria F. Maroulis

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Giobbi	
U.S. Patent No.: 9,298,905	Examiner: To Be Assigned
Issued: March 29, 2016	Art Unit: To Be Assigned
Application No.: 14/521,982	
Filed: October 23, 2014	
Title: BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION	**REQUEST FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510**

Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 35 U.S.C. § 302 and 37 C.F.R. §§ 1.510 et seq., Samsung Electronics America, Inc. ("Samsung" or "Requestor") requests *ex parte* reexamination of claims 1-18 (the "Challenged Claims") of U.S. Patent No. 9,298,905 ("the '905 patent," Exhibit 1001), entitled "Biometric Personal Data Key (PDK) Authentication." The '905 patent issued on March 29, 2016, from Application No. 14/521,982, which was filed on October 23, 2014.

Patent Owner has asserted the '905 patent against Samsung and Samsung's parent, Samsung Electronics Co., Ltd., in *Proxense, LLC v. Samsung Electronics Co., Ltd., et. al.*, Case No. 6:21-CV-00210-ADA (W.D. Tex.). Because the '905 patent is involved in concurrent litigation, the Patent Office should accord the requested reexamination "priority over all other cases." MPEP § 2261.

TABLE OF CONTENTS

Page

I. INTRODUCTION 19

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510 20

A. Payment of Fees – 37 C.F.R. § 1.510(a) 20

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1) 21

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2) 21

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3) 22

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4) 22

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5) 22

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6) 23

III. PROCEDURAL HISTORY 23

A. Prosecution History of the '905 Patent 24

B. The IPR filed against the '905 Patent 25

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES 25

V. LEVEL OF SKILL IN THE ART 28

VI. CLAIM CONSTRUCTION 29

A. "third party trusted authority" (claim 1) 30

VII. PRIORITY DATE OF THE '905 PATENT 31

VIII. OVERVIEW OF THE TECHNOLOGY 32

IX. OVERVIEW OF THE PRIOR ART 33

A. Ludtke (Ex. 1005) 33
B. Okereke (Ex. 1006) 35
C. Robinson (Ex. 1007) 36
D. Scott (Ex. 1008) 37
1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson 38
2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson 38
X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS 39
A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious 40
1. The Proposed Combination 40
(a) The Prior Art Discloses the Claim Limitations 40
(b) A POSITA Would be Motivated to Combine Ludtke and Okereke 42
2. Claim 1 46
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device" 46
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;" 49
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;" 52
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and 54

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 58

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 60

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 60

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 60

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 61

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 61

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 62

9. Claim 9: 63

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 63

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 63

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 63

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 64

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 64

12. Claim 13: 65

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 65

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 65

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code." 66

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 68

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 68

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 68

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 68

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious 68

1. The Proposed Combination....68
(a) The Prior Art Discloses the Claim Limitations....68
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke....69
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."....70
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code....71
C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious....71
1. The Proposed Combination....71
(a) The Prior Art Discloses the Claim Limitations....71
(b) A POSITA Would be Motivated to Combine Ludtke and Scott....74
2. Claim 1....79
(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"....79
(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"....81
(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"....82
(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and....82

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction." 82

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code." 83

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition." 83

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 83

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application." 83

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account." 84

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data." 84

9. Claim 9: 84

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;" 84

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and" 84

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third - party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction." 85

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network." 85

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob." 85

12. Claim 13: 86

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating

that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and" 86

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes." 86

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code." 87

14. Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob." 87

15. Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition." 87

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account." 88

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application." 88

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious 88

1. The proposed combination....88
(a) The Prior Art Discloses the Claim Limitations....88
(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott....89
2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code. 90
3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code. 91
XI. REAL PARTIES OF INTEREST 91
XII. CONCLUSION....91

TABLE OF ATTACHMENTS AND EXHIBITS

Attachments

(1) Certificate of Service to Patent Owner
(2) Ex. 1011 Form PTO/SB/08a (Information Disclosure Statement)

Exhibits

The '905 patent, Declaration, and Prosecution History

Ex. 1001	U.S. Patent No. 9,298,905 ("'905 patent")
Ex. 1002	File History of the '905 patent
Ex. 1003	Expert Declaration of Dr. Benjamin Goldberg
Ex. 1004	CV of Dr. Benjamin Goldberg

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Other

Ex. 1009	Decision Denying Institution of *Inter Partes* Review, Paper No. 12, IPR2021-01447 (February 28, 2022)
Ex. 1010	Claim Construction Order in *Proxense, LLP v. Samsung Electronics Co., Ltd*, Case No. 6:21-CV-00210 (W.D. Tex.) Dkt. 43.
Ex. 1011	Form PTO/SB/08a (Information Disclosure Statement)
Ex. 1012	Introduction to Public Key Technology
Ex. 1013	Security Issues for Contactless Smart Cards
Ex. 1014	Smart Card Alliance Web Site
Ex. 1015	Smart Card Alliance Contactless Payment and the Retail Point of Sale

LISTING OF CLAIMS

CLAIM	LIMITATION
1a	A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device;
1b	responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
1c	comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
1d	responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
1e	responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.
2	The method of claim 1, further comprising: registering an age verification for the user in association with the ID code.
3	3. The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code.

CLAIM	LIMITATION
4	4. The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
5	The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
6	The method of claim 1, wherein completing the financial transaction includes accessing an application.
7	The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
8a	The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification; and
8b	responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data.

CLAIM	LIMITATION
9a	An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;
9b	a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
9c	a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction.
10	The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network.
11	The integrated device of claim 7, wherein an age verification is registered in association with the ID code.
12	The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

CLAIM	LIMITATION
13a	A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and
13b	the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a comparison of the ID code received and the legitimate codes included in the list of the legitimate codes.
14	The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code.
15	The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.
16	The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal

CLAIM	LIMITATION
	scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.
17	The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.
18	The system of claim 11, wherein completing the financial transaction includes accessing an application.

I. INTRODUCTION

The challenged claims are directed to conventional technology to prevent unauthorized use of a wireless device by verifying both biometric information and the device itself. None of the concepts in the '905 patent were new when the patent was filed; they are clearly disclosed in prior art references that together disclose each and every element of the challenged claims. Moreover, all of the concepts in the patents were used for various different applications for years before the '905 patent was filed. Nevertheless, Patent Owner has launched a lawsuit against Samsung, alleging infringement of technology far newer and more innovative than the technology described in the challenged claims.

The lawsuit against Samsung involves five patents, all relating to similar technology. After the lawsuit against Samsung was filed, Samsung filed IPRs against all five asserted patents. Two of the IPRs were instituted (against US Patent Nos. 9,049,188 and 9,235,700) and are currently pending. The Board denied institution, however, on the '905 patent and two additional related family members: U.S. Patent Nos. 8,352,730 and 10,698,989. In the decisions not to institute the IPRs, the Board found merit in the Patent Owner's argument (which Samsung did not foresee, as it contradicted Patent Owner's claim construction arguments in litigation) that the prior art did not disclose a "third party trusted authority." The

present petition addresses Patent Owner's new argument with different prior art, and therefore presents substantial new questions of patentability.

This Request presents several substantial new questions of patentability. All four SNQs rely primarily on a new reference (Ludtke) that was cited neither during prosecution of either the '905 patent or any of its parents nor in the prior IPR petition regarding the '905 patent. Specifically, SNQ 1 relies on a combination of Ludtke and Okereke, neither of which was presented in the IPR. SNQ 2 relies on a third reference for a single limitation found in a handful of dependent claims. SNQs 3 and 4 rely on a combination of Ludtke and Scott, and while the Scott reference was presented in the IPR, it is cited here only as a secondary reference. Like SNQ 2, SNQ 4 relies on a third reference for a single limitation in a number of dependent claims. Respectfully, these combinations present substantial new questions of patentability that have not been considered by either the PTO or the PTAB.

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION UNDER 37 C.F.R. § 1.510

This request for *ex parte* reexamination of the '905 patent satisfies each requirement of 37 C.F.R. § 1.510.

A. Payment of Fees – 37 C.F.R. § 1.510(a)

Requestor authorizes the Patent and Trademark Office to charge Deposit Account No. DA505708 for the fees set in 37 C.P.R. § 1.20(c)(1) for reexamination.

B. Statement Pointing Out Each Substantial New Question of Patentability Based on Prior Art Patents and Printed Publications – 37 C.F.R. § 1.510(b)(1)

A detailed discussion of pertinent new teachings in the prior art references that present substantial new questions of patentability is provided in Section IX.

C. Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art – 37 C.F.R. § 1.510(b)(2)

Samsung respectfully requests reexamination of claims 1-18 of the '905 patent based on the following proposed rejections:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A detailed explanation of the pertinence and manner of applying the cited prior art to claims 1-18 of the '905 patent is provided in Section X.

D. Copies of the Cited Prior Art Presented- 37 C.F.R. § 1.510(b)(3)

A copy of every patent or printed publication relied upon as a basis of unpatentability are submitted as exhibits in conjunction with this request for reexamination. In addition, a Form PTO/SB/08a is attached hereto as Exhibit 1011. A full list of exhibits appears on page 11.

E. Copy of the Patent for Which Reexamination Is Requested- 37 C.F.R. § 1.510(b)(4)

A copy of the '905 patent is attached to this Request as Exhibit 1001.

F. Certification of Service on the Patent Owner- 37 C.F.R. § 1.510(b)(5)

The signature on this request certifies that a copy of the request has been served in its entirety on PO's representative at the address provided for in 37 C.F.R. § 1.33(c). Specifically, PO's representative was served by first-class U.S. mail on June 8, 2022, addressed to:

Patent Law Works/Proxense
Greg Sueoka
310 East 4500 South, Suite 400
Salt Lake City, UT 84107

The Requester has also provided courtesy copies to PO's counsel in the aforementioned litigation by first-class U.S. mail on June 8, 2022, addressed to:

Hecht Partners
David Hecht
125 Park Avenue, 25th Floor
New York, NY 10017

Susman Godfrey
Brian Melton
1000 Louisiana St, Suite 5100
Houston, TX 77002

G. Certification of Statutory Estoppel Provisions - 37 C.F.R. § 1.510(b)(6)

Samsung certifies that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) and 325(e)(1) do not prohibit it from filing this ex parte reexamination request.

Requestor previously filed one petition for *inter partes* review against the '905 patent. *See* IPR2021-01447. The petition was denied institution.

III. PROCEDURAL HISTORY

Requestor is unaware of any co-pending Patent Office proceedings involving the '905 patent. This is the first reexamination request challenging the claims of the '905 patent.

The '905 patent claims priority to two provisional patents: U.S. Patent Application Nos. 60/637,538, filed on Dec. 20, 2004, and 60/652,765, filed on Feb. 14, 2005. The '905 patent is a continuation of application no. 13/710,109, filed on Dec. 10, 2012 (now, U.S. Pat. No. 8,886,954), which is a continuation of application no. 11/314,199, filed on Dec. 20, 2005 (now, U.S. Pat. No. 8,352,730). The application that led to the '905 patent was filed on October 23, 2014. The '905 patent issued on March 29, 2016.

A. Prosecution History of the '905 Patent

The '905 patent was filed on October 23, 2014 and claimed the benefit of application no 60/637,538 filed on December, 2004. Ex. 1002 at 482-83, 486.

On June 12, 2015, after lengthy exchange regarding various formalities, the U.S. Patent & Trademark Office (hereinafter "Patent Office") issued the first non-final Office Action rejecting claims 2-18 under 35 U.S.C 103 in light of Hsu et al. (US 6,041,410) in view of Saito et all (US 20040129787) as well as non-statutory double patenting in light of US Patent No. 8,886,954. Ex. 1002 at 94-109.

After amendment and an examiner-initiated interview to suggest terminal disclaimers the Patent Office issued a Notice of Allowance on December 16, 2015. Ex. 1002 at 37-47 and 76-80.

B. The IPR filed against the '905 Patent

Samsung previously filed an IPR against the '905 patent. IPR2021-01447. The IPR presented four grounds. The first two grounds were based on the Scott reference, combined with others. The third ground was based on the Berardi reference in combination with others. The PTAB denied institution of the first two grounds based on its belief that none of the cited prior art disclosed a "third party trusted authority" with respect to claim 1. *See, e.g.*, IPR2021-01447, Paper 12 at 20-26. The PTAB denied institution on the third ground for unrelated reasons. *See, e.g.*, IPR2021-01447, Paper 12 at 27-30.

IV. THIS REQUEST SHOULD NOT BE DENIED BASED ON DISCRETIONARY ISSUES

Patent Owner may argue that this request should be denied in accordance with § 325(d) based on the Federal Circuit's decision in *In re Vivint, Inc.*, 14 F.4th 1342 (Fed. Cir. 2021). That case, however, does not apply here. In *Vivint*, the Requestor filed an *Ex Parte* Reexam request after filing a series of vexatious IPR petitions, the last of which the Board found was an "undesirable, incremental" attack on the Patent Owner. The Board reasoned that allowing such practices "risks harassment of patent owners and frustration of Congress's intent in enacting [the AIA]," and therefore denied the petition. *Id.* at 1346.

Notwithstanding that denial, the Requestor in *Vivint* filed a reexam request that ultimately resulted in cancellation of the challenged claims. On review, the Federal Circuit reversed the CRU's decision to grant the reexam, finding that the request, just like the denied IPR petition, was an abusive filing. The Federal Circuit noted that the vast majority of the reexam was a copy of the denied IPR petition, and the Court concluded that the Director's finding that the IPR petition was abusive should have likewise applied to the reexam request. Specifically, the Court found that the reexam "copied, word-for-word, two grounds from the [denied IPR petition]--the very petition deemed 'a case of undesirable, incremental petitioning.'" *Id.* at 1353. And, for the portions that were not copied, the EPR "used prior Board decisions as a roadmap to correct past deficiencies." *Id.*

The facts here are distinguishable. ***First***, and most importantly, Samsung's previous IPR petition was not a series of "serial" petitions that were "undesirable, incremental petitions." There was only a single prior IPR filed on the '905 patent.

Second, this request is not a "word-for-word" copy of the denied IPR petition. To the contrary, the first SNQ in this request includes *completely new* art that was not seen in either prosecution or the prior IPR. In all four SNQs presented in this reexam, the primary reference, Ludtke, is completely new and was not considered during prosecution or presented in the previously filed IPR. Although

the Scott reference was previously used in the prior IPR, it is used here only as a secondary reference in two SNQs. Similarly, the Robinson reference, which was used for a very specific limitation found in a handful of dependent claims, is also used for that same limitation in the dependent claims. Notably, the Board did not disagree that Robinson teaches that limitation.

Third, this reexam is not using the prior, denied '905 IPR petition as a "roadmap" to correct past deficiencies. In *Vivint*, the requestor copied, word-for-word, two grounds in their entirety, which the Board had already found to be vexatious harassment. Even in the portions that were not copied, the Board found that the same or similar prior art was used. Here, Samsung's request presents entirely new proposed SNQs of rejection. There are ***no*** SNQs that are "word-for-word" copies of the IPR grounds, and indeed, the primary reference that forms the vast basis for the rejections is entirely different and thus do not, and could not, use the prior IPR petition denial as a "roadmap."

Fourth, each of the above patents and publications are prior art to the Asserted Patents, and as mentioned above, the grounds of rejection outlined in this Request raise substantial new questions of patentability, because the reference combinations used to establish these grounds provide teachings not previously considered by the Office. None of the reference combinations used to establish the

grounds for rejection in this Request, nor the grounds themselves, were advanced by the Examiner during prosecution of the applications that matured into the Asserted Patents.

Further, the references are also non-cumulative because, as discussed in more detail below, the prior art reference individually and/or in combination disclose each and every limitation of the challenged claims—including the challenged independent claims that were allowed over the considered prior art.

For these reasons, the present request should not be denied pursuant to the CRU's discretionary powers.

V. LEVEL OF SKILL IN THE ART

The '905 patent claims priority to two provisional applications filed on December 20, 2004, and February 14, 2005. A person of ordinary skill in the art ("POSITA") at that time would have had a bachelor's degree in computer science or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). More education could compensate for less experience and vice versa. Ex. 1003 at ¶13. Each of the arguments below is made from the standpoint of a POSITA in the field of the '905 patent. Requestor's expert, Dr. Benjamin Goldberg, was at least a POSITA at the time of the alleged invention. *Id.*; Ex. 1004.

VI. CLAIM CONSTRUCTION

The USPTO construes claims in accordance with their "broadest reasonable interpretation" ("BRI") in light of the claim language and specification. *In re Reuter*, 670 F.2d 1015, 1019 (C.C.P.A. 1981); *In re Smith International, Inc.*, 871 F.3d 1375, 1381, 1382-83 (Fed. Cir. September 26, 2017). This is as true in reexamination proceedings as it is during original prosecution. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re ICON Health & Fitness, Inc.*, 496 F.3d 1374, 1379 (Fed. Cir. 2007). The USPTO broadly interprets claims during examination of a patent application because the applicant may "amend his claims, the thought being to reduce the possibility that, after the patent is granted, the claims may be interpreted as giving broader coverage than is justified." *In re Prater*, 415 F.2d 1393, 1404-05 (C.C.P.A. 1969). According to the Federal Circuit, "[t]his approach serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified. Applicants' interests are not impaired since they are not foreclosed from obtaining appropriate coverage for their invention with express claim language." *In re Yamamoto*, 740 F.2d 1569, 1571-72 (Fed. Cir. 1984) (*citing In re Prater*, 415 F.2d at 1405 n.31). The same policy underpinning the use of the broadest-reasonable-interpretation standard in initial examination, justifies its application in reexamination. *Id.*

Since the filing of the IPR, the District Court has issued a claim construction order construing terms as follows:

Claims	**Term**	**Construction**
1-3, 8-11,13-14	"ID code"	A unique code identifying a device
1, 9, 13	"access message"	A signal or notification enabling or announcing access

Ex. 1010 at 3. In addition to these terms, the Court also construed a number of terms as having their "plain meaning." *Id.* Although the terms above have been construed according to the *Phillips* standard, Requestor has applied these constructions in the discussion below, as the Broadest Reasonable Interpretation encompasses the *Phillips* standard. Accordingly, if the prior art meets the limitations construed according to the *Phillips* standard, it meets the limitations construed according to BRI.

A. "third party trusted authority" (claim 1)

In the previous IPR, the PTAB construed the term "third party trusted authority" as "an entity or party separate from the principal parties to a transaction." Ex. 1009, IPR2021-01447, Paper 12 at 13. In considering the prior art in light of its construction of the term, the PTAB found that Petitioner did not "explain[] sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application is being permitted to access in

the asserted combination." *Id.* at 24.[1] The Patent Owner argued that the DPC in Lapsley (which Petitioner pointed to as the "third party trusted authority") actually acted as a "cloud based digital wallet," and further that the purchaser did not access the digital wallet using a "fob" or "phone," but rather a device in the store where they were purchasing something. Ex. 1009 at p. 23-24. Based on these arguments, the PTAB found that the "the DPC is the resource to be accessed" and that "it is a party to the transaction, rather than a third party." *Id.* The PTAB further observed that during prosecution, the applicant explained that a "user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *Id.* at 24.

Requestor has applied this construction, in light of the Board's observations and analysis, to the prior art below.

VII. PRIORITY DATE OF THE '905 PATENT

The '905 patent claims priority to two provisional applications: U.S. Patent Application No. 60/637,538, filed December 20, 2004, and U.S. Patent Application No. 60/652,765, filed on February 14, 2005. Although Requestor does not concede that all 18 claims are entitled to one or both of the priority dates of the provisional

[1] Lapsley was the prior art reference that was relied upon for the "third party trusted authority" limitation in the IPR.

applications, all prior art references relied on in this petition date back to before December 20, 2004, and therefore, no further determination needs to be made regarding the priority date.

VIII. OVERVIEW OF THE TECHNOLOGY

The '905 patent relates to integrated wireless devices in a generic "computerized authentication" system that is used to gain access to devices, applications, or accounts through a biometric validation procedure. Ex. 1001 at 1:21-24, 1:49-54. The integrated device validates a user's biometric scan against biometric data stored on the device. *Id.* at 1:62-2:5. After validation using the biometric scan, a code stored on the device is transmitted to indicate that the user's identity has been verified. *Id.* The device transmits the code to a third-party trusted authority that determines if the code is authentic by checking it against a list of legitimate integrated device codes. *Id.* at 6:37-42. If the code is authentic, the user is allowed access to the device, application, or account they seek access to. *Id.* at 2:37-42. The '905 patent purports to solve for users the problem of having to "memorize or otherwise keep track of the[ir] credentials." *Id.* at 1:33-35. The patent also purports to solve the problem of illegitimate users "us[ing] a stolen access object to enter a secured location because the user's identity is never checked." *Id.* at 1:46-48.

IX. OVERVIEW OF THE PRIOR ART

A. Ludtke (Ex. 1005)

U.S. Patent No. 7,188,110 ("Ludtke") was filed on December 11, 2000. It issued on March 6, 2007. It is therefore prior art under 35 U.S.C. § 102(e) (pre-AIA).

Titled "Secure and Convenient Method and Apparatus for Storing and Transmitting Telephony-Based Data," Ludtke discloses a method of identifying an authorized user with a biometric device and enabling the authorized user to access private information. Ex. 1005 at Abstract. Ludtke recognizes both the need to ensure the integrity of financial information and the privacy of the user. *Id.* at 1:11-21.

The system disclosed in Ludtke is strikingly like the system disclosed in the '905 patent. The Ludtke system allows transactions through an eCommerce system through a "transaction device" that has a unique identifier (ID). *Id.* at 3:34-35. The transaction device can be a privacy card or a digital wallet or both. *Id.* at 3:35-39. This transaction device is a wireless device that is carried and maintained by a user. *See, e.g., id.* at 5:40-44. The transaction device includes a highly secured memory that can provide a transaction processing clearing house (TPCH) the necessary information to authorize a transaction. *Id.* at 3:40-45. The Ludtke system is described in Figure 1:

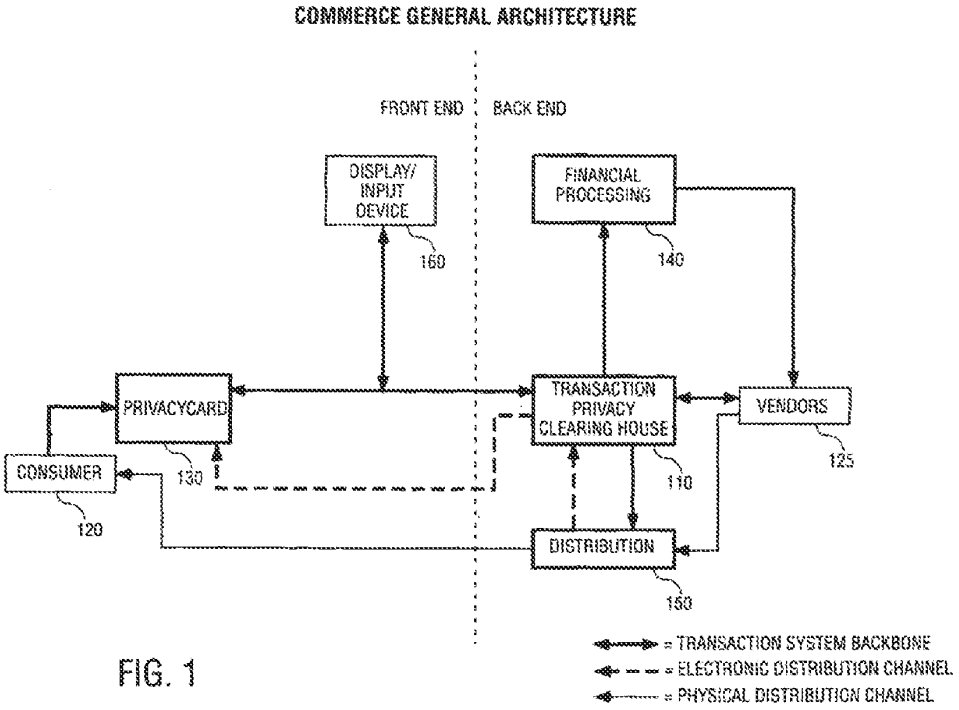


FIG. 1

As demonstrated in this figure, the Consumer 120 uses a transaction device 130 (in this figure, shown as a privacy card). The consumer wishes to purchase something from a vendor 125. The transaction device provides information to the TPCH for authorization for the transaction between the consumer and vendor to be performed. *Id.* at 6:36-44. The TPCH is not part of the transaction, but rather functions as a third-party middleman of the transaction. *Id.* at 7:44-46. This ensures that sensitive information is not shared with the vendor. *Id.* at 7:46-48.

Recognizing the need to protect the authorization of a user, Ludtke also discloses the use of fingerprint recognition as part of the digital wallet. *Id.* at 18:16-17. This biometric verification occurs before any transaction can take place, and therefore authorizes the user before the transaction device authorizes the device with the TPCH. *Id.* at 25:65-26:9; Ex. 1003 at ¶¶37-41.

B. Okereke (Ex. 1006)

U.S. Publication No. 2003/0196084 ("Okereke") was filed April 11, 2003. It published October 16, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

Okereke describes a "system and method for allowing users of wireless and mobile devices to participate in Public Key Infrastructure[PKI]" and also indicates that it "facilitates secure remote communications." Ex. 1006 at Abstract. Okereke states that "systems that perform electronic financial transactions or electronic commerce must protect against unauthorized access to confidential records and unauthorized modification of data." *Id.* at ¶3.

In setting up communications for a mobile device, Okereke specifically teaches that "a unique identifier for the wireless product to be employed is passed [sic] at 210 to the proxy server 125 program for authorization. The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other

device capable of remote wireless communication. The unique identifier can be a serial number or SIM." *Id.* at ¶25.

Okereke describes the PKI: "With PKI, a public and private key are created simultaneously using the same algorithm by a certificate authority. Information encrypted by the private key can only be decrypted with the corresponding public key. The private key is given only to the requesting party, and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the network." *Id.* at ¶ 7. Therefore, the private key is secret information. Ex. 1003 at ¶¶42-45.

C. Robinson (Ex. 1007)

U.S. Publication No. 2003/0177102 ("Robinson") was filed February 19, 2003. It published September 18, 2003. It is therefore prior art under 35 U.S.C. § 102(a) (pre-AIA).

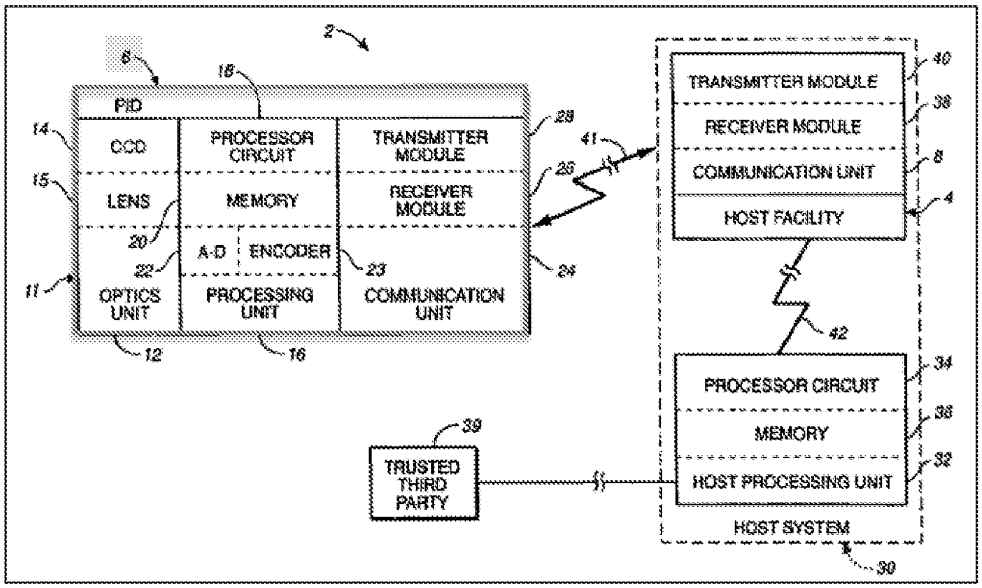
Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents

biometric and age-verifying information. *Id.* at ¶¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user; Ex. 1003 at ¶¶46-47.

D. Scott (Ex. 1008)

International PCT Application WO 99/56429 ("Scott") was filed on April 26, 1999. It was published on November 4, 1999. The International Publication Date is November 4, 1999, making it prior art under 35 U.S.C. § 102(b) (pre-AIA).

Scott discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1 [2]; Ex. 1003 at ¶48.

1. A POSITA Would Have Been Motivated to Combine the Teachings of the Ludtke, Okereke, and Robinson

Ludtke, Okereke, and Robinson all relate to protecting confidential information, communication over wireless networks, and the use of biometric information to protect this communication. All three references relate to communications for the purpose of financial transactions. Ex. 1005 at 4:54-56, 6:51-67; Ex. 1006 ¶3; Ex. 1007 ¶¶31-32, 47, Fig.1. A POSITA would naturally consider the teachings of Ludtke, Okereke, and Robinson in order to get a full understanding of the available options for secure communications and would have been motivated by this to combine the references' teachings. As explained in detail below, a POSITA would have considered applying the teachings of Okereke and Robinson to the teachings of Ludtke.

2. A POSITA Would Have Been Motivated to Combine the Teachings of Ludtke, Scott, and Robinson

Ludtke, Scott, and Robinson also relate to protecting confidential information over wireless networks, using biometric information to protect sensitive information, and also relates to financial information. Ex. 1005 at

[2] Annotations are added to figures unless indicated otherwise.

4:54-56, 6:51-67; Ex. 1007 ¶¶31-32, 47, Fig.1; Ex. 1008 at 10:24-32, 18:29-19:20. Therefore, a POSITA would have combined the Scott reference with Ludtke and Robinson for the same reasons above with respect to Okereke. In fact, a POSITA would have considered all of these references in trying to develop a process of secure communications.

X. DETAILED EXPLANATION OF THE PROPOSED REJECTIONS

As shown in detail below, claims 1-18 of the '905 patent are unpatentable under 35 U.S.C. § 103 in light of the prior art references and combinations of references presented below. The following rejections should be adopted in their entirety:

SNQ 1: Ludtke in combination with Okereke renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 2: Ludtke in combination with Okereke and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102 (a) and (e) and 35 U.S.C. § 103;

SNQ 3: Ludtke in combination with Scott renders obvious claims 1, 3-10, and 12-18 under 35 U.S.C. §§ 102 (b) and (e) and 35 U.S.C. § 103; and

SNQ 4: Ludtke in combination with Scott and Robinson renders obvious claims 2 and 11 under 35 U.S.C. §§ 102(a), (b), and (e) and 35 U.S.C. § 103.

A. SNQ 1: Ludtke in combination with Okereke Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 1 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

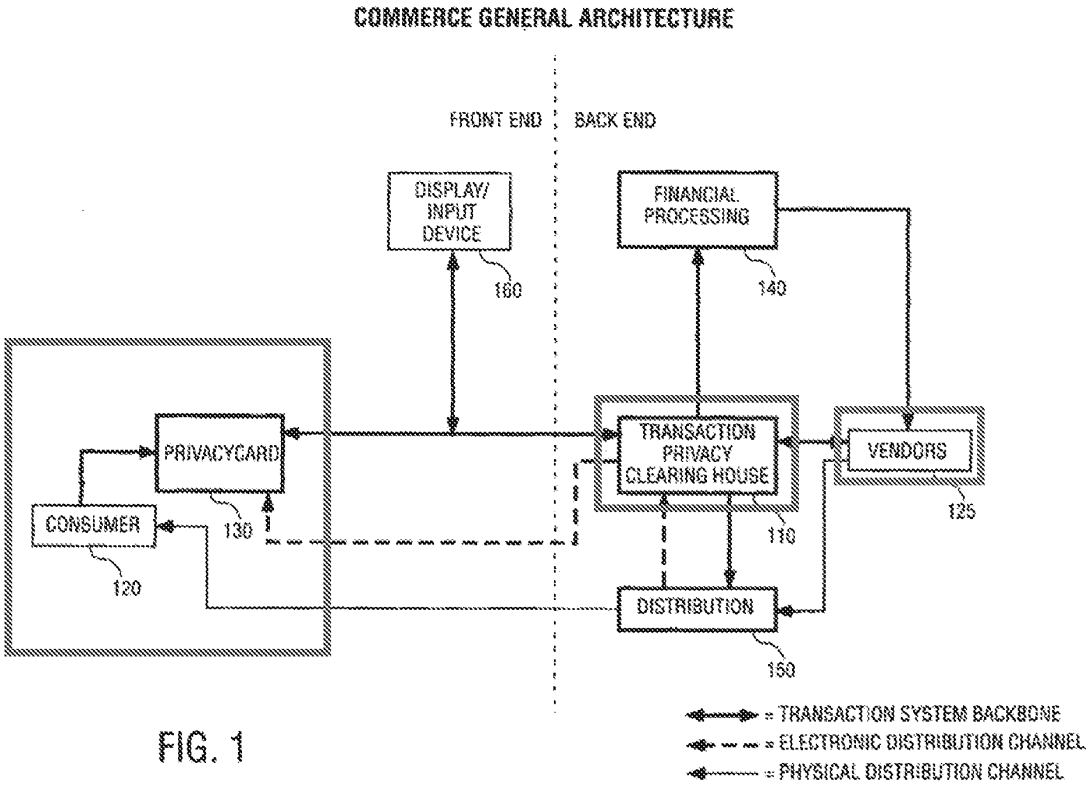


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information. Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third-party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Okereke discloses this "secret information."

Specifically, Okereke discloses a "secret key" that is maintained by the user, and can be used to encrypt and decrypt information communicated to the user. Ex. 1006 at ¶ 25.

The claims also require an "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Okereke, however, does disclose this device ID code information, in the form of a unique serial number or SIM number for the user device. *Id*; Ex. 1003 at ¶¶196-198.

(b) A POSITA Would be Motivated to Combine Ludtke and Okereke

The scope and content of the prior art would have motivated a POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique" nature of a device ID.

Ludtke discloses a persistent, tamper-proof memory, and a POSITA would have been motivated to combine the secret key disclosed in Okereke with the system disclosed in Ludtke. Ex. 1003 at ¶¶ 199-206. A POSITA would have

already known, as of the priority date of the '905 patent, that encryption using a secret key such as that as part of PKI would have been obvious when communicating confidential information. *Id.*

POSITAs specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* Public Key Cryptography, which later developed into PKI encryption years before the '905 patent, was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* POSITA would therefore recognize that the use of PKI encryption, which is disclosed in Okereke, would make the system of Ludtke even more secure. *Id.* Okereke simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a

financial transaction. A POSITA would have combined the teachings of Okereke's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or a SIM. Ex. 1003 at ¶¶199-206. Okereke explicitly discloses this fundamental information. Ex. 1006 at ¶25.

A POSITA would have been motivated to combine Ludtke and Okereke because they are both in the same field of endeavor. *Id.* Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a user and device, including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ex. 1005 at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Ex. 1006 at Title ("System and method for secure wireless communication using PKI"); *id.* ¶31 ("In order to begin using the system via wireless device, the user may be required to provide

additional forms of authentication to the CPS, such as password or biometric signature.").

A POSITA would also have reasonably expected the combination of Ludtke and Okereke to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Given this disclosure in Ludtke, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret information in Ludtke's memory and using the unique device ID disclosed in Okereke as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use PKI-compliant encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number or SIM, and would have expected this combination to succeed. Ex. 1003 at ¶¶199-206.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the PKI-compliant encryption system because it had long been used as a way to encrypt and decrypt information and

share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Okereke in the Ludtke system to further complement Ludtke's features. *Id.*

2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

Ludtke and Okereke disclose this limitation.

An integrated device, biometric data, and an ID code: Ludtke discloses an integrated device, *e.g.*, Ludtke's "transaction device." Ex. 1005 at 3:32-35. Ludtke's transaction device provides a number of different "integrated" functions, including maintaining bills and bill paying on the device (*id.* at 4:4-6), online shopping (*id.* at 4:7-35), and downloading and accessing electronic catalogs (*id.* at 4:36-39). The transaction device includes a number of hardware options such as a magnetic stripe generator (*id.* at 3:49-51), a screen (*id.* at 55-57), and a bar code reader (*id.* at 3:61-63).

Ludtke explains that the "transaction device enhances security by ***authenticating the user of the card prior to usage***..." *Id.* at 4:62-65. This authentication can be performed by PIN code entry, or by other technologies such

as a biometric solution. *Id.* at 4:65-5:1. The biometric information ensures that the user is indeed legitimate.

Ludtke also specifically discloses authentication of a device through the use of "transaction device information." *Id.* at 6:36-44. A POSITA would recognize that this transaction device information necessarily includes unique device IDs, such as serial numbers and SIMs. Ex. 1003 at ¶¶208-212. But this knowledge of a POSITA is further embedded within Okereke. *See* Ex. 1005 at 6:36-44, *see also* Ex. 1006 at ¶30. As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Okereke.

Okereke also discloses a method for verifying a user during authentication of an integrated device. Okereke discloses wireless and mobile devices which are integrated devices. Ex. 1006 at Abstract. "The wireless product 165 can be a personal digital assistant (PDA), laptop, cellular telephone or any other device capable of remote wireless communication." *Id.* at ¶25.

Okereke specifically discloses authenticating the wireless device. Okereke describes a proxy server program awaiting initiation to establish secure wireless access capabilities. *Id.* at ¶25. When authentication is requested, "a unique identifier for the wireless product to be employed is passed as at 210 to the proxy server 125 program for authorization." *Id.* "The unique identifier can be a serial number or

SIM number, for example." *Id.* Both serial numbers and SIM numbers are unique codes that identify the devices they are attached to. Ex. 1003 at ¶¶208-212. A POSITA would recognize that a serial number or SIM number is a unique identifier of a mobile device. *Id.* Once the proxy server confirms the unique identifier, it authorizes the device by sending approval to a desktop computer to make a key exchange to allow communication. *Id.*

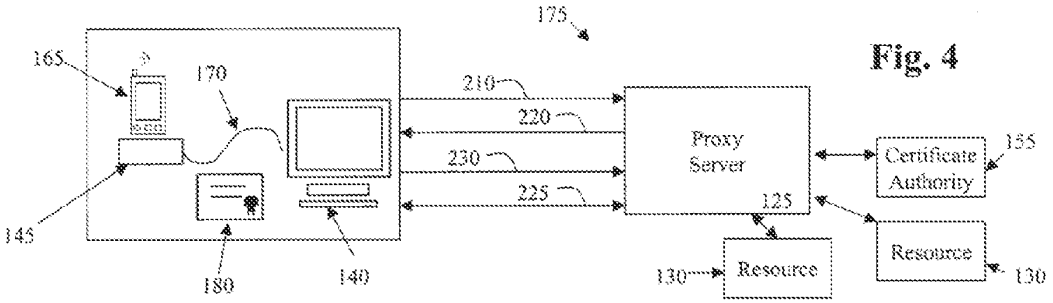


Fig. 4

Persistently storing biometric information and an ID code: Ludtke discloses a persistent storage on the integrated device. Specifically, the transaction device disclosed in Ludtke includes a process to use fingerprint data (biometric data of the user) to secure the device. Ludtke describes persistently storing the fingerprint data on the integrated device:

> The fingerprint data entry process may be performed at least twice, to confirm that the user has entered the correct data (using the correct fingerprint). If confirmation succeeds, the device writes the fingerprint image data into write once memory, or other memory that is protected from accidental modification.

Id. at 19:35-40. This fingerprint data is persistently stored in a tamper-proof format that is unable to be subsequently altered (write-once memory or other memory that is protected from accidental modification). Indeed, a write-once memory will only allow writing once, therefore, the information cannot be tampered with, and cannot be modified. Ex. 1003 at ¶213. In each case, this memory is persistent storage, because the information stored is not easily re-writable. *Id.*

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

Ludtke describes receiving scan data from a biometric scan responsive to receiving a request for a biometric verification of the user. As explained above, Ludtke describes using biometric verification – including a fingerprint – to verify the user of the device. Figure 28 shows a device with a Fingerprint Identification Unit (FIU) 2806 and a touchpad 2808 for user input:

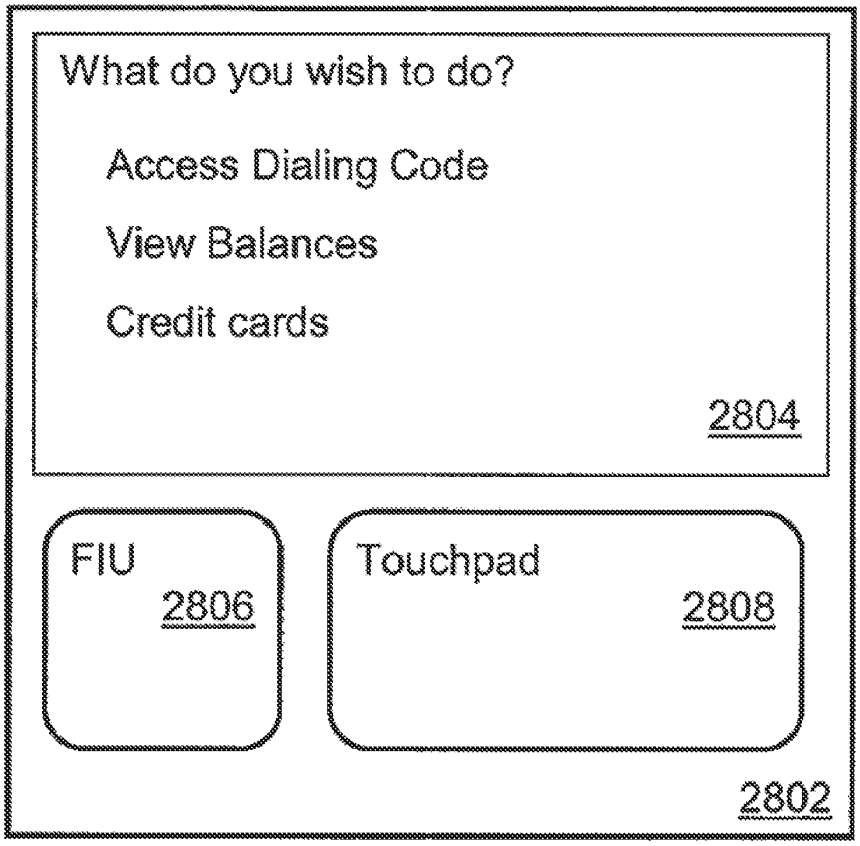


FIG. 28

Ex. 1005 at Fig. 28. "The user of the consumer access device 2802 would be authorized access to the device 2802 if the device recognized the user after the user had pressed his finger against the FIU 2806." *Id.* at 39:24-27.

A POSITA would recognize that FIU 2806 is a "biometric sensor." Ex. 1003 at ¶215. Indeed, the only way the FIU would be able to detect the fingerprint – and

determine the data present in the fingerprint – is if it was a fingerprint (or biometric) sensor. *Id.*

Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

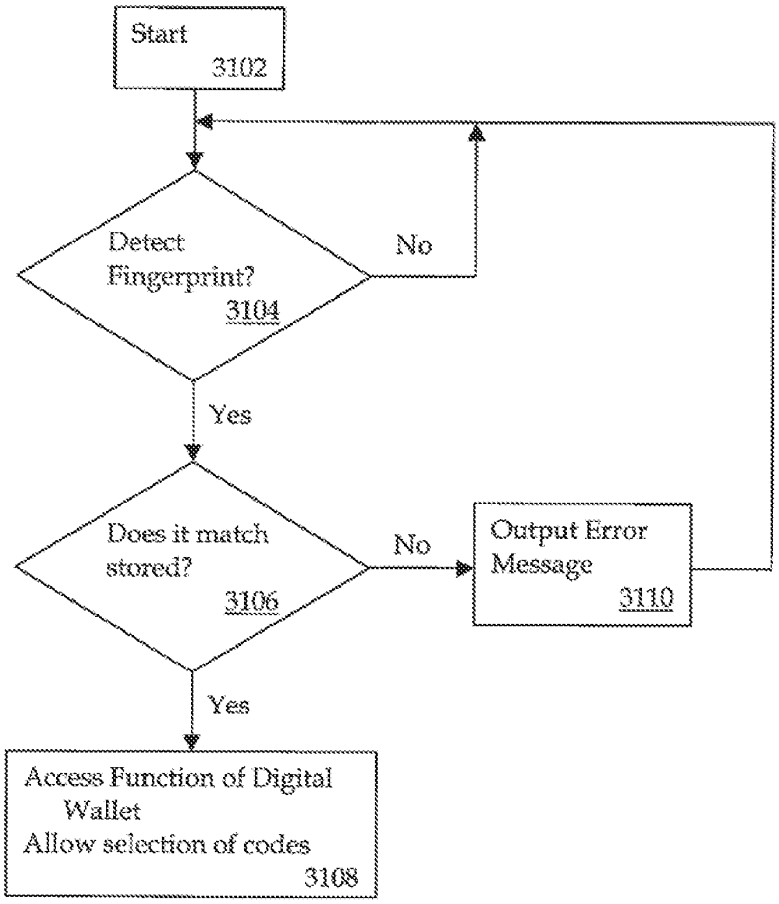


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, the device is continuously looking for a request for verification ("Detect fingerprint"). In response to that request, it will receive scan data from the touchpad so it can determine whether the fingerprint matches (3106). *Id.* at 39:47-59.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

Ludtke also shows this limitation in Figure 31:

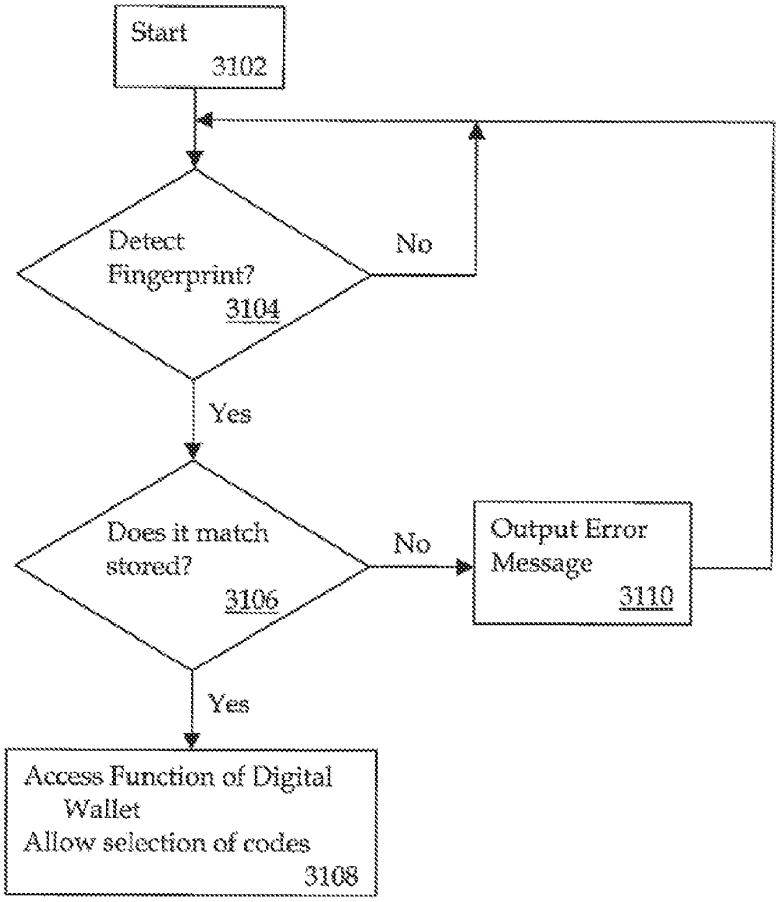


FIG. 31

Ex. 1005 at Fig. 31. Ludtke explains that if "a fingerprint has been detected, then at 3106 a check is made to see if it matches a stored authorized fingerprint. If a match does not occur, then at 3110 an error message is output and the DW [Digital Wallet/Integrated Device] returns to checking to see if a fingerprint has been

detected 3104. If the fingerprint does match a stored one, then at 3108 the DW allows access to functions of the DW and access to a selection of codes." *Id.* at 39:47-54.

(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

Responsive to a determination that the scan data matches the biometric data: As explained in conjunction with limitation [1c], if the scanned fingerprint data matches the stored fingerprint, then access to functions of the integrated device, such as the digital wallet, is permitted. *Id.* at 39:47-54.

Third party trusted authority: Ludtke describes a transaction processing [or privacy] clearing house (TCPH) which is a third party trusted authority. The TPCH "may access relevant account information to authorize transactions." *Id.* at 3:40-45. Figure 1 of Ludtke shows how the TPCH is a third party:

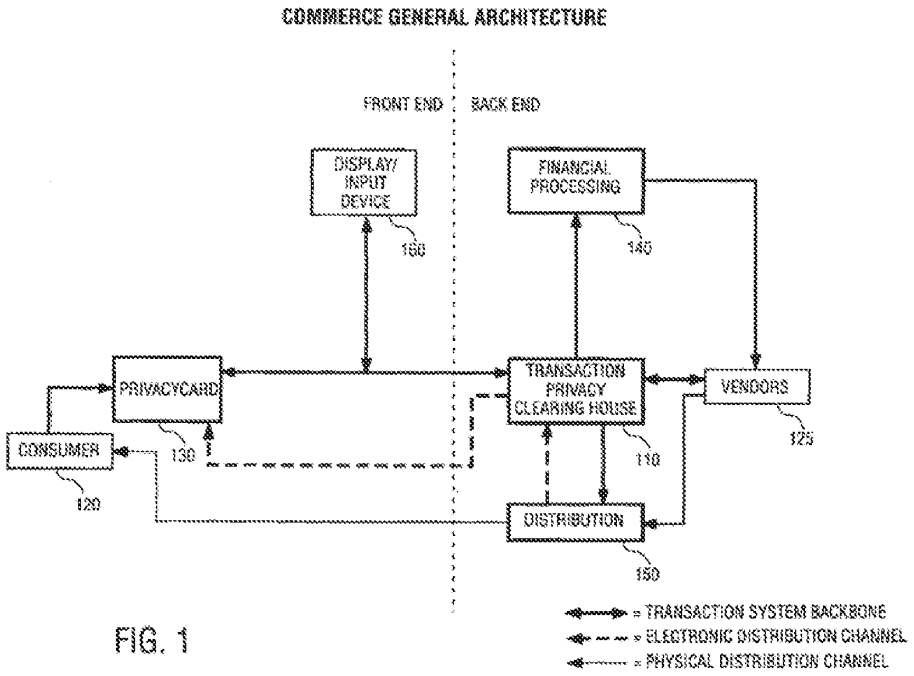


FIG. 1

Ex. 1005 at Figure 1. Figure 1 shows the commerce general architecture. *Id.* at 6:36-8:24. Figure 1 shows a consumer 120 who wishes to complete a purchase, *id.* at 6:36-64, and a vendor 125, who is selling something to the user 120. *Id.* "In this embodiment, a transaction privacy clearing house (TPCH) 110 interfaces a user 120 and a vendor 125." *Id.* at 6:36-38.

The TPCH is a third party to the transaction between the user/consumer 120 and the vendor 125. Ludtke explains that in "one embodiment of electronic distribution, the TPCH 110 functions as the middleman of the distribution channel.

This allows TPCH 110 to retain user privacy by not exposing addressing information and possibly email addresses to third parties." *Id.* at 7:44-48. This demonstrates that the TPCH acts as a middleman to ensure that only necessary information is exchanged between the consumer 120 and the vendor 125, but is not associated with either of them.

The TPCH is also a "trusted authority." Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. The consumer 120 and vendor 125 therefore trust the TPCH to indicate whether the transaction may be complete. Ex. 1003 at ¶¶ 219-221.

Wirelessly sending the ID code: Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42; Ex. 1003 at ¶222.

One or more previously registered ID codes maintained by the third-party trusted authority: Ludtke also explains that the "TPCH 110 maintains a secure database of transaction device information and user information. In one embodiment, the TPCH 110 interfaces to at least one financial processing system 140 to perform associated financial transactions, such as confirming sufficient funds to perform the transaction, and transfers to the vendor 125 the fees required to complete the transaction." *Id.* at 6:49-55. And as explained above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Therefore, the TPCH includes previously registered information that can be compared with information from the consumer and the consumer's device so the TPCH can determine whether the consumer 120 is authorized to complete a transaction with vendor 125. Indeed, the transaction device information that the TPCH compares to the received transaction device information must be stored within the TPCH as a list of codes (and specifically, a list of ID codes), in order to perform the comparison function that is disclosed. *Id.* at 30:19-27; Ex. 1003 at ¶223.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure

database by the TPCH 110. *Id.* at 6:41-44. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Okereke, and would have recognized that the "transaction device information" would include a device serial number or SIM code, both of which uniquely identify the integrated device. Ex. 1003 at ¶224.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction."

As indicated above, Ludtke explains that the "transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 ***and the user 120*** approval of the transaction to be performed." Ex. 1005 at 6:41-44. A POSITA would recognize that when the TPCH 110 "indicates to . . . the user 120," that indication is in the form of an access message allowing the user access to an application. Ex. 1003 at ¶225. In this case, the TPCH is allowing access to the application on the transaction device that will permit the transaction to be completed. Specifically, the TPCH is sending a signal (or a notification) to the user's device, which allows (it enables or announces) access to the application on the transaction device that will permit the transaction to be completed. Ludtke further discloses this limitation at Fig. 15, Step 1520:

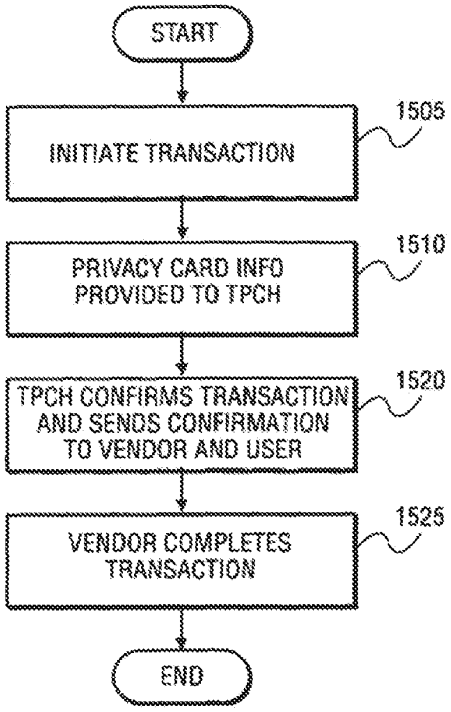


FIG. 15

Ex. 1005 at Fig. 15, *see also* Fig. 17, steps 8 and 9-1. With regard to step 1520, Ludtke teaches that the "TPCH, at step 1520, confirms the transaction and provides the confirmation to the vendor and the user. At step 1525, the vendor completes the transaction without the knowledge of the user." *Id.* at 27:13-16. The transaction, as described in Ludtke, is a financial transaction because it is a purchase from a vendor by the user. Ex. 1003 at ¶225.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

Ludtke and Okereke disclose this limitation. As explained above, Ludtke discloses the transaction device receiving biometric information allowing access to the device and then subsequently communicates the ID code to the TPCH. Ex. at 1003 at ¶226. It is inherent that, when the ID code is sent to the TPCH, that is an indication that the biometric verification has been successful. Indeed, as the ID code will not be sent at all if biometric verification fails (Ex. 1005 at 19:35-45), the sending of the ID code itself is an "indication that the biometric verification was successful." *Id.*

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

Ludtke describes a number of different types of biometric information that may be used: "The identification by the biometric device may be achieved in a variety of ways, as discussed above. For example, biometric identification, may be, ***fingerprint***, ***retinal scan***, ***voice***, DNA, ***hand profile***, ***face recognition***, etc." Ex. 1005 at 35:60-64; Ex. 1003 at ¶227.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet,

laptop, mp3 player, mobile gaming device, watch and a key fob."

Ludtke and Okereke disclose this limitation. POSITA would recognize that the transaction device disclosed in Ludtke, which includes a number of different iterations, including a privacy card (Ex. 1005 at 20:43-50), and a cellular telephone mechanism (*id.* at 17:3-10), would meet many of these limitations including "mobile phone," "tablet," and "key fob." Okereke explicitly states that its device may be a mobile phone. Ex. 1006 at Abstract; Ex. 1003 at ¶228.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as an application and files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶229.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

Ludtke discloses this limitation. In Ludtke, access would be given applications of either computer software, a file (or both). In a number of

embodiments, Ludtke describes the transaction device as including a "digital wallet" which POSITA would recognize as files that allow a user to digitally store credit card and other payment information and to make transactions with that card. Ex. 1005 at 5:1-5; Ex. 1003 at ¶230. Moreover, a POSITA would recognize that giving access to the digital wallet is providing access to a financial account. *Id.*; Ex. 1003 at ¶230.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

Ludtke and Okereke disclose this limitation. For example, Ludtke discusses the process of requesting and receiving biometric information. *See supra* Section X.A.2; Ex. 1005 at 39:19-35. Ludtke then describes an embodiment where the biometric information is not needed: "Alternatively, the consumer access device, once the user has been identified may not require re-identification until the consumer access device is, for example, turned off." *Id.* at 39:35-38. A POSITA would recognize that in this embodiment, a request to authenticate the device for a financial transaction after biometric verification had occurred, but before the device was turned off is a request to send the ID code without an additional biometric

verification. Ex. 1003 at ¶231. A POSITA would recognize that in this case, the ID code would be sent without biometric verification. *Id.*

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

See Claim 1, element [1a]. Section X.A.2.a, *supra*; Ex. 1003 at ¶232.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and"

See Claim 1, elements [1c], [1d]. Section X.A.2.c, d, *supra*.

The "validation module" will be the portion of the smartphone, including processors and instructions that receives the scan and verifies the biometric information. Ex. 1003 at ¶234. A POSITA would recognize that the validation module would be in coupled with the memory, since the biometric information that the validation module compares with received biometric information is stored in the memory for comparison. *Id.*

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based

on the comparison of the ID code and allowing the user to—complete a financial transaction."

See Claim 1, elements [1d], [1e]. Section X.A.2.d, e, *supra*. A POSITA would recognize that because the transaction device has wireless access, it necessarily has a "radio frequency communication module," as all wireless communications occur through an RF module. Ex. 1003 at ¶235.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

Ludtke and Okereke disclose this limitation. As explained above, Ludtke explains that "[t]he transaction device information is provided to the TPCH 110 that then indicates to the vendor 125 and the user 120 approval of the transaction to be performed." *Id.* at 6:41-44. Ludtke also explains that "the transaction device may contain wireless data communication," and may also "closely resemble a standard credit card." *Id.* at 5:36-41. In describing the TPCH specifically, Ludtke indicates that a "variety of communication devices may be used, such as the Internet, direct dial-up modem connections, wireless or cellular signals, etc." *Id.* at 9:35-42. Therefore, the communications described above in conjunction with claim 1 (by both Ludtke and Okereke) to the agent are transmitted over a network. Ex. 1003 at ¶236.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

See Claim 5. Section X.A.5, *supra*; Ex. 1003 at ¶237.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

See Claim 1, elements [1a], [1d], [1e]. Section X.A.2.a, d-e, *supra*. The integrated devices described above are hardware devices because they are held by the user. Ex. 1003 at ¶238. The "authentication circuit" is the portion of the hardware device, including processors and instructions that receives the scan and verifies the biometric information. *Id.*

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

See Claim 1, elements [1d], [1e]. Section X.A.2.d-e, *supra*; Ex. 1003 at ¶239.

13. Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."

See Claim 1, elements [1b], [1c]. Section X.A.2.b-c, *supra*. Figure 31 describes the process to verify a user of the integrated device (described in this embodiment as a digital wallet):

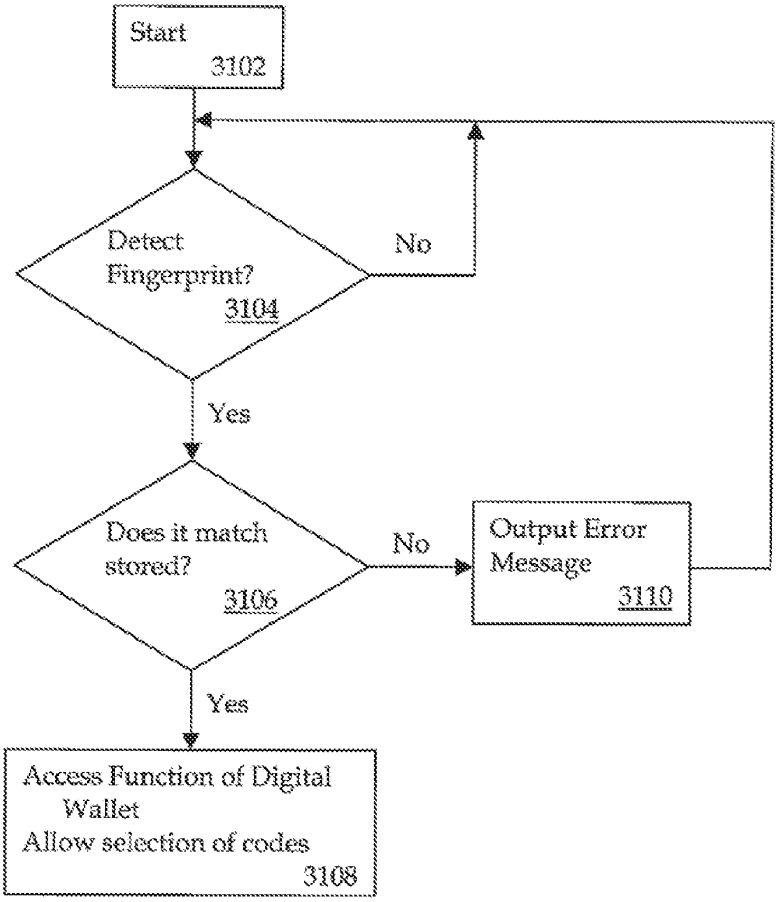


FIG. 31

Id. at Fig. 31. As can be seen in the flow chart, if the scan data does not match the stored data (i.e., the device cannot authenticate the user), it will output an error message, and not allow access to the digital wallet or selection of codes. *Id.* at 39:47-59. Ex. 1003 at ¶¶240-241.

14. **Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."**

See claim 5, section X.A.5, *supra*; Ex. 1003 at ¶242.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition, and a voice recognition."**

See claim 4, Section X.A.4, *supra*; Ex. 1003 at ¶243.

16. **Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."**

See claim 7, Section X.A.7, *supra*; Ex. 1003 at ¶244.

17. **Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."**

See claim 6, Section X.A.6, *supra*; Ex. 1003 at ¶245.

B. SNQ 2: Ludtke in combination with Okereke and Robinson Renders Claims 2 and 11 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 2 relies entirely on Ludtke and Okereke for the same reasons as outlined in SNQ 1, but also relies on Robinson for the limitations in dependent claims 2 and 11. Both of these dependent claims involve registering an age

verification. Where Ludtke and Okereke do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Okereke. Ex. 1003 at ¶246.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Okereke

The scope and content of the prior art would have motivated POSITA to combine Robinson with Ludtke and Okereke. Ex. 1003 at ¶¶247-250. Like both Ludtke and Okereke, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. *Id.* at ¶9-10; Ex. 1003 at ¶¶247-250. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in Robinson would, for example, allow a way for the Ludtke system to ensure that the user is

old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. *Id.*

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. *Id.* Robinson, like Ludtke and Okereke, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Okereke to also include the age of the user who was verified with biometric information. *Id.* The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the ID code."

Ludtke in combination with Okereke disclose all of the limitations of claim 1. *See* SNQ 1, Claim 1. Section X.A.2, *supra.*

However, neither Ludtke nor Okereke expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses that a central database 102 holds information related to users to authenticate a user's age to access an age restricted area, for example. Ex. 1007 at ¶¶27-28, 32, 66-67, Fig. 1. The central database 102 stores age verification records related to individuals seeking age verification (called "presenters"), including information such as a

user's age, date of birth, government ID number, biometric template, and at least one ID number that identifies the presenter within the system. *Id.* Prior to using the age-verification system, an individual presents biometric and age-verifying information. *Id.* at ¶13-15. Robinson further discloses that age-verifying information is associated with at least one ID number (SID) identifying the user. Ex. 1003 at ¶252.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the ID code.

Ludtke in combination with Okereke disclose all of the limitations of claim 9. *See* SNQ 1, Claim 9. Section X.A.9, *supra*; Ex. 1003 at ¶253.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.B.2, *supra*. Ex. 1003 at ¶254.

C. SNQ 3: Ludtke in combination with Scott Renders Claims 1, 3-10, and 12-18 Obvious

1. The Proposed Combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 3 relies on Ludtke as the base reference, which discloses a mobile device used for performing financial transactions. Ludtke discloses all of the limitations in claims 1, 3-10, and 12-18 except the "unique Device ID" and storage

of "secret information." Specifically, Ludtke discloses the system as shown below in figure 1:

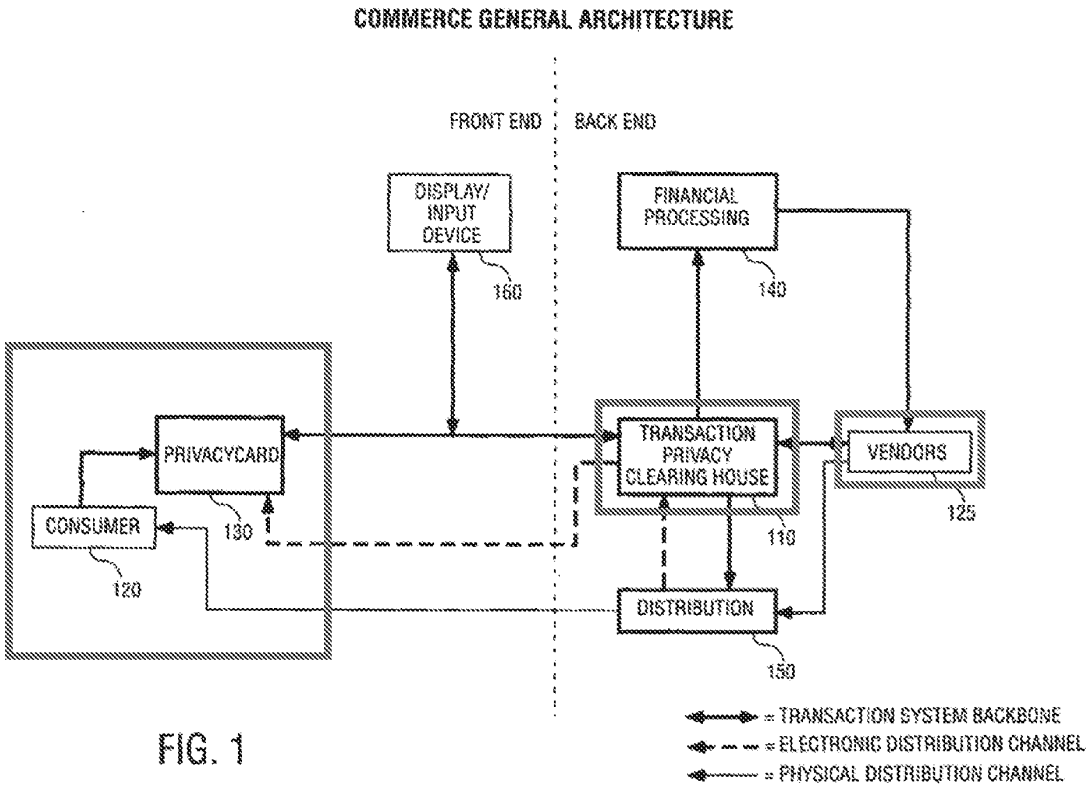


FIG. 1

Figure 1 shows one embodiment of the system in Ludtke. Ludtke discloses a "transaction device," which is seen above as the Privacy Card 130. Ex. 1005 at 6:36-44, Fig. 1. The transaction device is a device that the consumer 120 uses and includes a number of embodiments, including a privacy card, and digital wallet. *Id.* at 5:1-5, 11-14, 6:36-44. The transaction device also authorizes the consumer 120 using biometric data, including a fingerprint and other biometric information.

Ludtke's transaction device includes and discloses a persistent, tamper proof storage. Ludtke also discloses the process to authenticate a financial transaction between the consumer 120 and a vendor 125. The financial transaction is authorized through the transaction privacy clearing house 110, which is a third party, independent of the consumer 120 and the vendor 125. Ludtke emphasizes the third party aspect of the transaction privacy clearing house 110 because the third party ensures that private information is not exchanged between the consumer 120 and the vendor 125. *Id.* at 6:45-49, 29:43-53.

The claims require storage of "secret information" in the user's device. Although Ludtke does not explicitly disclose this "secret information," it does disclose (1) a storage location for this information, (*id.* at 10:46-49, 24:61-65), as well as (2) the importance of maintaining the confidentiality of private information (*id.* at 3:45-47; 5:30-31, 6:45-49). Scott discloses this "secret information." Specifically, Scott includes an extensive discussion regarding a secret key infrastructure. Scott discloses that the device's memory 20 also stores a private key unique to each device and used for encryption, which can be "set into memory by the manufacturer." Ex. 1008 at 11:24-30, 28:13-15, 4:14-18. Scott discloses that this "private key" used by the PID 6 is never disclosed. *Id.* at 8:21-22.

The claims also require a unique "ID code" that identifies the user's device that is communicated to the third party trusted authority for authorization of the device. Ludtke discloses "transaction device information" that is communicated from the consumer's transaction device 130 to the transaction privacy clearing house 110 for authorization, but Ludtke does not explicitly indicate that this "transaction device information" is unique. Scott, however, does disclose a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further 10 store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. Serial numbers are unique codes that identify the devices that they are attached to. Ex. 1003 at ¶¶255-258. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

(b) A POSITA Would be Motivated to Combine Ludtke and Scott

The scope and content of the prior art would have motivated POSITA to combine Ludtke and Okereke. As explained above, Ludtke discloses almost all of the limitations of the claims except for "secret information" and the "unique"

nature of a device ID code. Similar to Ludtke, Scott discloses authenticating a user using a "personal identification device" (PID) for protected applications such as opening a hotel room door or a conducting a point-of-sale transaction. *Id.* at 8:5-12. Scott specifically describes a system for authentication of a mobile device to protect information for financial transactions. *Id.* at 2:5-16.

Ludtke discloses a persistent, tamper proof memory, and POSITA would have been motivated to combine the secret key disclosed in Scott with the system disclosed in Ludtke. Ex. 1003 at ¶¶259-265. The secret key infrastructure disclosed in Scott is similar to that disclosed in Okereke, as discussed above. *Id.* As discussed above, a POSITA would have already known, as of the priority date of the '905 patent, that encryption using a secret key such as that disclosed in Scott would have been obvious when communicating confidential information. *Id.* A POSITA specifically recognized the importance of encrypted communication when engaging in communications regarding financial information and especially when authenticating financial transactions. *Id.* The use of secret information (such as that in PKI encryption) to perform this type of encryption was well-known ***decades*** before the filing date of the '905 patent, and was a well-established, well-known method for implementing encryption. *Id.* For example, Public Key Cryptography, which later developed into PKI encryption years before the Challenged Patents,

was developed in the 1970s, and serves as a well-known way to encrypt and authenticate secret or confidential information. *Id.* A POSITA recognized that such encryption is important to many applications, including financial information where it is particularly important to keep the information secret. *Id.* A POSITA would therefore recognize that the use of secret information, which is disclosed in Scott, would make the system of Ludtke even more secure. *Id.* Scott simply demonstrates this knowledge prior to the '905 patent's priority date.

Ludtke discloses transaction device information communicated between the transaction device and the transaction privacy clearing house for authorization of a financial transaction. A POSITA would have combined the teachings of Scott's unique Device ID with Ludtke's system. As discussed above, Ludtke explicitly teaches communication of "transaction device information" with the TPCH. Ex. 1005 at 6:38-51. A POSITA would have recognized that such transaction device information necessarily includes unique device identifiers such as a serial number or other number that is specific to the processing unit. Ex. 1003 at ¶¶259-265. Scott explicitly discloses this fundamental information. *Id.*

A POSITA would have been motivated to combine Ludtke and Scott because they are both in the same field of endeavor. Indeed, both references are in the same field of endeavor as the '905 patent, *i.e.*, authentication of a device,

including use of biometric information, for the purpose of exchanging sensitive information over a network. *See* Ex. 1001 at 1:21-24 ("The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated"); Ludtke at Abstract ("A method of identifying an authorized user with a biometric device and enabling the authorized user to access private information over a voice network is disclosed"); Scott at Abstract ("A portable, hand-held personal identification device (6) and method for providing secure access to a host facility…"); *id.* ¶31 ("Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility").

A POSITA would have reasonably expected the combination of Ludtke and Scott to succeed and yield predictable results. Ludtke's system already discloses a persistent and tamper-proof memory and discusses the use of sensitive information. Ludtke also discloses transaction device information. Ex. 1005 at 6:38-51. Scott similarly discloses a persistent, tamper-proof memory. Scott teaches that data is stored in a memory where, after biometric enrollment, "there is no going back or editing." Ex. 1008 at 16:11-12. Given these disclosures, a POSITA would have expected the combination to result in Ludtke's financial system storing the secret

information in Ludtke's memory and using the unique device ID disclosed in Scott as the transaction device information. A POSITA would have expected this to yield the predictable result of the option to use secret key encryption and decryption with a private key (secret information), as well as the ability to ensure authentication of an authorized device using unique device identifying information such as a serial number, and would have expected this combination to succeed. Ex. 1003 at ¶264.

For example, Ludtke describes a protected memory to keep the type of important and sensitive information described in Okereke. Ex. 1005 at 19:37-40. Moreover, a POSITA would be familiar with the secret key encryption system because it had long been used as a way to encrypt and decrypt information and share such information only for authorized users. Implementing such a system with Ludtke would have been logical and obvious to a POSITA. Finally, both systems have similar types of mobile devices, and have similar goals. It would make sense to a POSITA to use the type of information identified in Scott in the Ludtke system to further complement Ludtke's features. Ex. 1003 at ¶265.

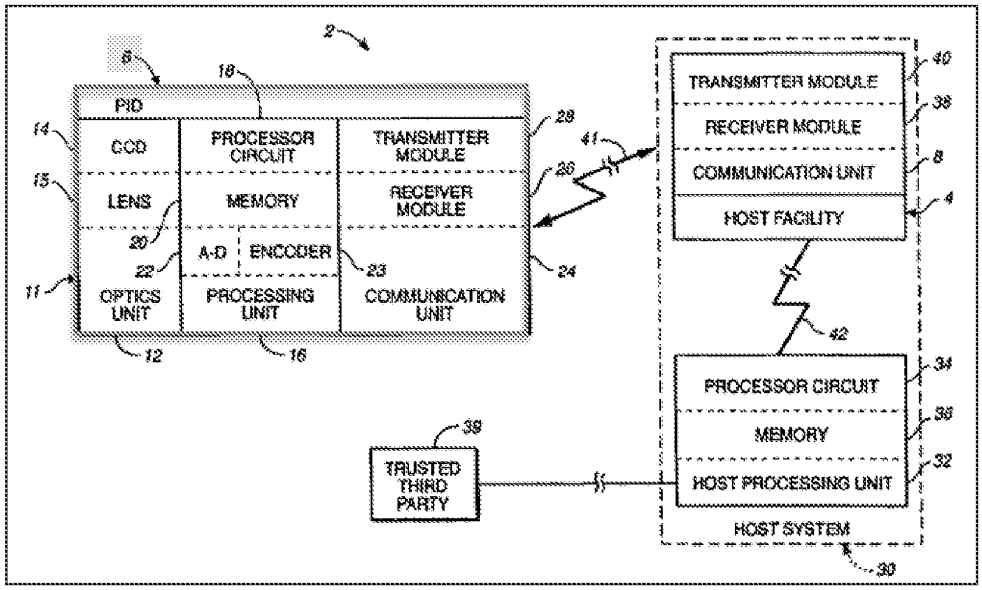
2. Claim 1

(a) [1a] "A method comprising: persistently storing biometric data of a legitimate user and an ID code on an integrated device"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.a, *supra*.

As explained above in detail, a POSITA would have been motivated to combine the disclosure of Ludtke with the disclosure in Scott.

Scott also discloses a method for verifying a user during authentication of an integrated device (*e.g.*, personal identification device ("PID") 6), in order to, for example, provide secure access to protected resources such as a hotel room or a point-of-sale transaction. Ex. 1008 at Abstract, 2:5-23, 4:22-5:9, 7:24-8:12; *see* claims [1A]-[1H] *infra*.



Ex. 1008 at Fig. 1.

As explained above, Scott discloses that the memory 20 of the PID 6 persistently stores a plurality of codes and other data values including a unique ID code that identifies the PID 6. Ex. 1008 at 4:9-10 ("The memory can further store an ID code indicative of the enrolled person or the device."), 8:13-22, 11:14-20. Specifically, memory 20 stores information "specific to processing unit 16," including a unique ID code that identifies the device, which may be set by the device manufacturer and can be the device serial number. *Id.* at 11:11-13. A serial number is a unique code that identifies the device it is attached to. Ex. 1003 at ¶¶267-270. Scott also discloses wherein the PID 6 stores other data values such as "a synchronization counter associated with the user device." *Id.* at 6:28-7:23, 13:10-15, 19:30-32.

As discussed above, a POSITA would have been motivated to modify the system of Ludtke to incorporate the unique serial numbers also disclosed in Scott. Ex. 1003 ¶¶267-270; *see supra* §X.C.1. A POSITA would have been motivated to store permanent information, such as the unique device identifiers (serial number). Moreover, a POSITA would have recognized that the "transaction device information" disclosed within Ludtke could further include the unique device information in Scott, which would ensure that the information used to authenticate the device only identifies the authorized device. *Id.* A POSITA would also have stored the unique device identifiers in the persistent tamper-proof memory, because this is important information that allows authorization and sensitive communications to take place, and a POSITA would have recognized the need to take care to ensure it is not easy to tamper with and modify the information. *Id.* at ¶270.

(b) [1b] "responsive to receiving a request for biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.b, *supra*. Ex. 1003 at ¶271.

(c) [1c] "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.c, *supra*. Ex. 1003 at ¶272.

(d) [1d] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.d, *supra*; Ex. 1003 at ¶273.

ID Code: Ludtke does not describe the specific "transaction device information" that is provided to the TPCH 110 and that is maintained in a secure database by the TPCH 110. Ex. 1005 at 6:36-64. However, as discussed above, a POSITA would have been motivated to combine Ludtke with the teachings of Scott, and would have recognized that the "transaction device information" would include a unique serial number, which uniquely identifies the integrated device. Ex. 1008 at 4:1-14, 5:10-21; Ex. 1003 at ¶274.

(e) [1e] "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully

authenticated the ID code, allowing the user to complete a financial transaction."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.2.e, *supra*; Ex. 1003 at ¶275.

3. Claim 3: "The method of claim 1, wherein an indication that the biometric verification was successful is sent with the ID code."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.3, *supra*. Ex. 1003 at ¶276.

4. Claim 4: "The method of claim 1, wherein the biometric data includes data from one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.4, *supra*. Ex. 1003 at ¶277.

5. Claim 5: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.5, *supra*. Ex. 1003 at ¶278.

6. Claim 6: "The method of claim 1, wherein completing the financial transaction includes accessing an application."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.6, *supra*. Ex. 1003 at ¶279.

7. Claim 7: "The method of claim 1, wherein completing the financial transaction includes accessing one or more of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.7, *supra*. Ex. 1003 at ¶280.

8. Claim 8: "The method of claim 1, further comprising: responsive to determining the action does not require biometric verification, receiving a request for the ID code without a request for biometric verification, and responsive to receiving the request for the ID code without a request for biometric verification, sending the ID code for authentication without requesting the scan data."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.8, *supra*. Ex. 1003 at ¶281.

9. Claim 9:

(a) [9a] "An integrated device comprising: a persistent storage media that persistently stores biometric data of a user and an ID code;"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.a, *supra*. Ex. 1003 at ¶282.

See also Claim 1, element [1a]. Section X.C.1.a, *supra*.

(b) [9b] "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends the ID code for comparison by a third-party trusted authority against

one or more previously registered ID codes maintained by the third-party trusted authority; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.b, *supra*. Ex. 1003 at ¶284.

See also Claim 1, elements [1c], [1d]. Section X.C.1.c, d, *supra*. Ex. 1003 at ¶285.

(c) [9c] "a radio frequency communication module that receives an access message from the third-party trusted authority indicating that the third -party trusted authority successfully authenticated the ID code sent to the third-party trusted authority based on the comparison of the ID code and allowing the user to—complete a financial transaction."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.9.c, *supra*. Ex. 1003 at ¶286.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d, e, *supra*. Ex. 1003 at ¶287.

10. Claim 10: "The integrated device of claim 7, wherein the ID code is transmitted to the third-party trusted authority over a network."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.10, *supra*. Ex. 1003 at ¶288.

11. Claim 12: "The integrated device of claim 7, wherein the integrated device comprises one or more of a mobile phone,

tablet, laptop, mp3 player, mobile gaming device, watch, and a key fob."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.11, *supra*. Ex. 1003 at ¶289.

See also Claim 5. Section X.C.5, *supra*. Ex. 1003 at ¶290.

12. Claim 13:

(a) [13a]. "A system, comprising: an integrated hardware device that persistently stores biometric data of a legitimate user and an ID code in the integrated hardware device, and that wirelessly sends the—ID code; an authentication circuit that receives the ED [sic- ID] code and sends the ID code to a third-party trusted authority for authentication, and that receives an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the ID code and allows the user to complete a financial transaction; and"

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.a, *supra*. Ex. 1003 at ¶291.

See also Claim 1, elements [1a], [1d], [1e]. Section X.A.1.a, d-e, *supra*. Ex. 1003 at ¶292.

(b) [13b]. "the third-party trusted authority operated by a third party, the third-party trusted authority storing a list of legitimate codes and determining the authentication of the ID code received based on a

comparison of the ID code received and the legitimate codes included in the list of the legitimate codes."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.12.b, *supra*. Ex. 1003 at ¶293.

See also Claim 1, elements [1d], [1e]. Section X.A.1.d-e, *supra*. Ex. 1003 at ¶294.

13. **Claim 14: "The system of claim 11 wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from a user to generate scan data and, when the integrated hardware device cannot verify the scan data as being from the legitimate user, the integrated hardware device does not send the ID code."**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.13, *supra*. Ex. 1003 at ¶295.

See Claim 1, elements [1b], [1c]. Section X.A.1.b-c, *supra*. Ex. 1003 at ¶296.

14. **Claim 15: "The system of claim 11, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."**

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.14, *supra*. Ex. 1003 at ¶297.

See also claim 5, section X.C.5, *supra*. Ex. 1003 at ¶298.

15. **Claim 16: "The system of claim 11, wherein the biometric data includes data based on one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a**

facial recognition, a signature recognition, and a voice recognition."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.15, *supra*. Ex. 1003 at ¶299.

See also claim 4, Section X.C.4, *supra*. Ex. 1003 at ¶300.

16. Claim 17: "The system of claim 11, wherein completing the financial transaction includes accessing one or more of a casino machine, keyless lock, an ATM machine, a web site, a file and a financial account."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.16, *supra*. Ex. 1003 at ¶301.

See also claim 7, Section X.C.7, *supra*. Ex. 1003 at ¶302.

17. Claim 18: "The system of claim 11, wherein completing the financial transaction includes accessing an application."

The disclosure of Ludtke for this limitation is described above in SNQ 1. Section X.A.17, *supra*. Ex. 1003 at ¶303.

See also claim 6, Section X.A.6, *supra*. Ex. 1003 at ¶304.

D. SNQ 4: Ludtke in combination with Scott and Robinson Renders Claims 2 and 11 Obvious

1. The proposed combination

(a) The Prior Art Discloses the Claim Limitations

SNQ 4 relies entirely on Ludtke and Scott for the same reasons as outlined in SNQ 3, but also relies on Robinson for the limitations in dependent claims 2 and

11. Both of these dependent claims involve registering an age verification. Where Ludtke and Scott do not explicitly disclose registering an age verification, Robinson discloses the age verification in claims 2 and 11. As explained below, a POSITA would be motivated to combine the age verification disclosed in Robinson with the system disclosed in Ludtke with the secret information and unique device ID disclosed in Scott. Ex. 1003 at ¶¶305-307.

(b) A POSITA Would have been Motivated to Combine Robinson with Ludtke and Scott

The scope and content of the prior art would have motivated a POSITA to combine Robinson with Ludtke and Scott. Ex. 1003 at ¶¶308-311. Like both Ludtke and Scott, Robinson discloses a way to improve security and to authenticate a user and device. Ex. 1007 at ¶¶27-29, 32, 66-67, Fig. 1.

All three of the references are therefore in the same field of endeavor, with Robinson specifically teaching improving security with an additional age-based authorization factor and to authenticate a user for age-restricted access or transactions initiated by a wireless device like Ludtke's transaction device. Ex. 1007 at ¶9-10; Ex. 1003 at ¶¶308-311. A POSITA would have recognized that the disclosure of Ludtke welcomes this modification with its stated aim to provide, for example, secure access to restricted areas. Ex. 1005 at 2:5-8, 10:24-28. Indeed, a POSITA would have recognized that the age verification disclosed in

Robinson would, for example, allow a way for the Ludtke system to ensure that the user is old enough to conduct a transaction, access a specific financial system or application, or to enter a restricted area. Ex. 1003 at ¶310.

A POSITA would also have had a reasonable expectation of success because age verification as disclosed in Robinson is a logical extension of the type of information that is exchanged. Ex. 1003 at ¶311. Robinson, like Ludtke and Scott, also discloses the use of biometric information to verify a user. Ex. 1007 at ¶39. It would be logical to modify the system of Ludtke and Scott to also include the age of the user who was verified with biometric information. Ex. 1003 at ¶¶308-311. The age would logically be registered at Ludtke's TPCH, where the age can also be kept confidential from third parties, consistent with Ludtke's goals. *Id.*

2. Claim 2: "The method of claim 1, further comprising: registering an age verification for the user in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 1. *See* SNQ 3, Claim 1. Section X.C.2, *supra*. Ex. 1003 at ¶312.

However, neither Ludtke nor Scott expressly disclose "registering an age verification for the user" as recited in this limitation. Robinson discloses this limitation as described in SNQ 2. *See* Section X.B.2; *see also* Ex. 1003 at ¶313.

3. Claim 11: "The integrated device of claim 7 [sic – 9], wherein an age verification is registered in association with the device ID code.

Ludtke in combination with Scott disclose all of the limitations of claim 9. *See* SNQ 3, Claim 9. Section X.C.9, *supra*. Ex. 1003 at ¶314.

Robinson in combination with Ludtke and Okereke disclose all of the limitations of claim 11 for the same reasons as described in conjunction with claim 2. Section X.D.2, *supra*. Ex. 1003 at ¶315.

XI. REAL PARTIES OF INTEREST

Requestor certifies that Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. are the real parties-in-interest.

XII. CONCLUSION

For at least the reasons cited herein, the prior art references cited in this Request present substantial new questions of patentability with respect to the Challenged Claims of the '905 patent. Accordingly, the Office should declare a reexamination of these claims and reject them on at least the SNQs detailed in this Request.

DATED: June 8, 2022

Respectfully submitted,

By *__/s/ Marissa Ducca*
QUINN EMANUEL URQUHART & SULLIVAN, LLP

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street NW, Suite 900
Washington, DC 20005
Email: marissaducca@quinnemanuel.com
Phone: (202) 538-8000
Fax: (202) 538-8100

James M. Glass (Reg. No. 46,729)
Quinn Emanuel Urquhart & Sullivan, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Email : jimglass@quinnemanuel.com
Phone: 212-849-7142
Fax: 212-849-7100

Attorneys for Third-Party Requestor Samsung Electronics America, Inc.

Trials@uspto.gov
571-272-7822

Paper No. 19
Entered: September 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GENERAL PLASTIC INDUSTRIAL CO., LTD.,
Petitioner,

v.

CANON KABUSHIKI KAISHA,
Patent Owner.

Case IPR2016-01357 (Patent 9,046,820 B1)[1]
Case IPR2016-01358 (Patent 9,046,820 B1)
Case IPR2016-01359 (Patent 8,909,094 B2)
Case IPR2016-01360 (Patent 8,909,094 B2)
Case IPR2016-01361 (Patent 8,909,094 B2)

Before DAVID P. RUSCHKE, *Chief Administrative Patent Judge*, SCOTT R. BOALICK, *Deputy Chief Administrative Patent Judge*, and JAMESON LEE, MICHAEL R. ZECHER, THOMAS L. GIANNETTI, JENNIFER S. BISK, and SHEILA F. McSHANE, *Administrative Patent Judges*.

McSHANE, *Administrative Patent Judge*.

DECISION
Denying Petitioner's Requests for Rehearing
37 C.F.R. § 42.71(d)

---

[1] These proceedings have not been joined or consolidated. Rather, because of the presence of common issues and the involvement of the same parties, we enter one Decision on Rehearing for these identified proceedings.

I. INTRODUCTION

General Plastic Industrial Co., Ltd., (hereafter "Petitioner") filed respective Requests for Rehearing of each of the Decisions Denying Institution of *inter partes* review in the following five related proceedings: (1) IPR2016-01357; (2) IPR2016-01358; (3) IPR2016-01359; (4) IPR2016-01360; and (5) IPR2016-01361.[2] In each Request for Rehearing, Petitioner contends that the corresponding Decision Denying Institution should be withdrawn, and *inter partes* review should be instituted. Also, in each Request for Rehearing, Petitioner requests that the panel on rehearing be expanded.

For purposes of this Decision on Rehearing, we treat the Request for Rehearing in IPR2016-01357 as representative, and specifically discuss the circumstances of that request. This discussion, however, equally applies to all the Requests for Rehearing. For ease of reference, unless otherwise indicated, all citations are to filings in IPR2016-01357, including the Request for Rehearing ("Req. Reh'g") and the Decision Denying Institution ("Dec."). Where appropriate, we add specific discussions pertaining to the other proceedings.

To summarize, and as discussed further below, Petitioner filed a first set of petitions seeking *inter partes* review of U.S. Patent No. 9,046,820 B1 ("the '820 patent") and U.S. Patent No. 8,909,094 B2 ("the '094 patent"). For each petition, institution of a trial was denied based upon the merits. Nine months after the filing

[2] The Decisions Denying Institution are listed as follows: IPR2016-01357 (Paper 16); IPR2016-01358 (Paper 12); IPR2016-01359 (Paper 12); IPR2016-01360 (Paper 12); and IPR2016-01361 (Paper 12). The Requests for Rehearing are listed as follows: IPR2016-01357 (Paper 17); IPR2016-01358 (Paper 13); IPR2016-01359 (Paper 13); IPR2016-01360 (Paper 13); and IPR2016-01361 (Paper 13).

of the first set of petitions, Petitioner filed follow-on petitions against the same patents. For each of those follow-on petitions, we exercised our discretion not to institute pursuant to 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a).

Petitioner alleges that trials should have been instituted on the follow-on petitions because a petitioner is not limited to filing just one petition per challenged patent under either 35 U.S.C. § 311 or § 314. Req. Reh'g 5. Petitioner also argues that we should not have relied on § 314(a), which, according to Petitioner, does not apply to the later petitions, and that we should have performed our analysis under 35 U.S.C. § 325(d). *Id.* at 5–7, 13–14. Furthermore, Petitioner alleges that in our analysis, we misapplied the factors set forth in the Board's *NVIDIA*[3] decision. Specifically, Petitioner contends that: (1) the factor of the limited one-year time period for issuing a final written decision should be afforded additional, if not dispositive, weight in light of the legislative history; (2) we abused our discretion by requiring that the prior art "should have been known" at the time the initial petitions were filed; and (3) we erred in considering potential prejudice to Patent Owner because the *NVIDIA* decision does not list such a factor. *Id.* at 6–13. Petitioner also requests that an expanded panel be designated. *Id.* at 14–15.

For the reasons that follow, we *deny* Petitioner's Requests for Rehearing.

[3] *NVIDIA Corp. v. Samsung Elec. Co.*, Case IPR2016-00134 (PTAB May 4, 2016) (Paper 9) (hereinafter, "*NVIDIA*").

II. DISCUSSION

A. Requests for an Expanded Panel

Our governing statutes and regulations do not permit parties to request, or panels to authorize, an expanded panel. *See generally* 35 U.S.C. § 6; 37 C.F.R. §§ 41.1–42.412; *see also AOL Inc. v. Coho Licensing LLC*, Case IPR2014-00771, slip op. at 2 (PTAB Mar. 24, 2015) (Paper 12) ("[P]arties are not permitted to request, and panels do not authorize, panel expansion."). Our standard operating procedures, however, provide the Chief Judge with discretion to expand a panel to include more than three judges. PTAB SOP 1, 1–3 (§§ II, III) (Rev. 14); *see id.* at 1 (introductory language explaining that the Director has delegated to the Chief Judge the authority to designate panels under 35 U.S.C. § 6); *see also In re Alappat*, 33 F.3d 1526, 1532 (Fed. Cir. 1994) (providing that Congress "expressly granted the Commissioner the authority to designate expanded Board panels made up of more than three Board members."). The Chief Judge may consider panel expansions upon a "suggestion" from a judge, panel, or party in a post-grant review. *Id.* at 3–4; *see also Apple Inc. v. Rensselaer Polytechnic Inst.*, Case IPR2014-00319, slip op. at 2 n.1 (PTAB Dec. 12, 2014) (Paper 20) (expanded panel) (per curiam).

The standard operating procedure exemplifies some of the reasons for which the Chief Judge may expand a panel. PTAB SOP 1, 3 (§ III.A). For example, an expanded panel may be appropriate when "[t]he proceeding or AIA Review involves an issue of exceptional importance." *Id.* (§ III.A.1).

In these cases, the Chief Judge has considered whether expansion is warranted, and has decided to expand the panel due to the exceptional nature of the

issues presented.[4] As we discuss further below, follow-on petitions have been at issue in multiple cases before the Board. The Chief Judge has determined that an expanded panel is warranted to provide a discussion of factors that are considered in the exercise of the Board's discretion under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a).

B. Requests for Rehearing

A party requesting rehearing has the burden to show a decision should be modified by specifically identifying all matters the party believes were misapprehended or overlooked, and the place where each matter was addressed previously in a motion, opposition, or a reply. 37 C.F.R. § 42.71(d). When rehearing a decision on institution, we review the decision for an abuse of discretion. 37 C.F.R. § 42.71(c). An abuse of discretion may arise if a decision is based on an erroneous interpretation of law, if a factual finding is not supported by substantial evidence, or if the decision represents an unreasonable judgment in weighing relevant factors. *Star Fruits S.N.C. v. United States*, 393 F.3d 1277, 1281 (Fed. Cir. 2005); *Arnold P'ship v. Dudas*, 362 F.3d 1338, 1340 (Fed. Cir. 2004); *In re Gartside*, 203 F.3d 1305, 1315–16 (Fed. Cir. 2000).

We present background on the cases below, and then address the arguments made by Petitioner in the Requests for Rehearing.

[4] As provided for in the standard operating procedure, and considering the commonality of issues considered here, the Judges on the initial panels in all the cases at issue have been designated as part of the expanded panel, and the Chief Judge and Deputy Chief Judge have been added to the panel. PTAB SOP 1, 4 (§ III.E).

1. Background

Petitioner initially filed a first set of petitions challenging the '820 patent and the '094 patent. The '820 and '094 patents generally relate to toner supply containers used with image forming apparatuses, and the challenged claims at issue in both patents are very similar. *Compare* Ex. 1001, 24:6–61, *with* IPR2015-01954, Ex. 1001, 24:15–25:5. Below is a summary of the proceedings corresponding to the first set of petitions.

'820 Patent Case

Case	Claims at Issue	Prior Art Asserted
IPR2015-01966 ("First '820 Patent Petition")	1, 7–9, and 16	Matsuoka[5]

'094 Patent Case

Case	Claims at Issue	Prior Art Asserted
IPR2015-01954 ("First '094 Patent Petition")	1, 7–9, 16–18, 29, and 38	Matsuoka

Petitioner filed these two petitions ("first-filed petitions") challenging claims of the '820 and '094 patents in September 2015. We denied institution of an *inter partes* review in those two proceedings based upon the merits of the challenges on March 9, 2016. *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, Case IPR2015-01966 (PTAB March 9, 2016) (Paper 9); *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, Case IPR2015-01954 (PTAB March 9, 2016) (Paper 9).

[5] U.S. Patent No. 5,903,806, issued May 11, 1999.

IPR2016-01357 (Patent 9,046,820 B1)
IPR2016-01358 (Patent 9,046,820 B1)
IPR2016-01359 (Patent 8,909,094 B2)
IPR2016-01360 (Patent 8,909,094 B2)
IPR2016-01361 (Patent 8,909,094 B2)

Petitioner filed Requests for Rehearing in those two proceedings, and those Requests were denied on May 19, 2016.

In July 2016, Petitioner filed two follow-on petitions in Cases IPR2016-01357 and IPR2016-01358, again challenging claims of the '820 patent, and three follow-on petitions in Cases IPR2016-01359, IPR2016-01360, and IPR2016-01361, again challenging claims of the '094 patent. The five follow-on petitions, and their designation by Petitioner ("Second," "Third," and "Fourth"), are summarized below.

'820 Patent Case

Case	**Claims at Issue**	**Prior Art Asserted**
IPR2016-01357 ("Second '820 Patent Petition")	1, 7–9, and 16	Suzuki[6], Ikesue[7], and Yasuda[8]
IPR2016-01358 ("Third '820 Patent Petition")	1, 7–9, and 16	Yoshiki[9], Koide[10], Kato[11], Matsuoka, and Ikesue

[6] Japan Patent Pub. No. 2000-305346, published November 2, 2000.
[7] U.S. Patent No. 5,598,254, issued January 28, 1997.
[8] U.S. Patent No. 5,481,344, issued January 2, 1996.
[9] U.S. Patent No. 5,765,079, issued June 9, 1998.
[10] Japan Patent App. No. H10-171230, published June 26, 1998.
[11] U.S. Patent No. 6,118,951, issued September 12, 2000.

'094 Patent Cases

Case	Claims at Issue	Prior Art Asserted
IPR2016-01359 ("Second '094 Patent Petition")	1, 7–9, and 29	Suzuki and Ikesue
IPR2016-01360 ("Third '094 Patent Petition")	1, 7–9, and 29	Yoshiki, Koide, Kato, Matsuoka, and Ikesue
IPR2016-01361 ("Fourth '094 Patent Petition")	1, 7–9, 11, 16–18, 29, and 38	Yasuda

In Patent Owner's Preliminary Responses to the follow-on petitions, Patent Owner argued that the Board should apply the factors set forth in the *NVIDIA* decision and deny the Petitions pursuant to 35 U.S.C. § 314(a). Paper 8, 4–10. Petitioner was granted leave to file Replies (Paper 10) to address issues arising under 35 U.S.C. §§ 314(a) and 325(d). Petitioner filed Replies to the Preliminary Responses (Paper 11) ("Reply"), and Patent Owner filed Sur-Replies in response to the Replies (Paper 13).

2. Decisions Denying Institution

We declined to institute *inter partes* reviews based on the follow-on petitions in Cases IPR2016-01357, IPR2016-01358, IPR2016-01359, IPR2016-01360, and IPR2016-01361 by exercising our discretion pursuant to 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a). *See, e.g.*, Dec. 12; *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, Case IPR2016-01360 (PTAB Nov. 14, 2016) (Paper 12) (hereinafter, "Dec. IPR2016-01360").

In exercising our discretion to deny each of the follow-on petitions, we considered seven factors, first set forth in *NVIDIA*, slip. op. at 6–7. In *NVIDIA*, the

Board determined that, when exercising discretion to deny institution of an *inter partes* review, we may consider the following factors:

1. whether the same petitioner previously filed a petition directed to the same claims of the same patent;
2. whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;[12]
3. whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition;[13]
4. the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;
5. whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;
6. the finite resources of the Board; and

[12] *See Conopco, Inc. v. Proctor & Gamble Co.*, Case IPR2014-00506, slip op. at 4 (PTAB Dec. 10, 2014) (Paper 25) (informative) (hereinafter, "*Conopco*"), and slip op. at 6 (PTAB July 7, 2014) (Paper 17); *Toyota Motor Corp. v. Cellport Sys., Inc.*, Case IPR2015-01423, slip op. at 8 (PTAB Oct. 28, 2015) (Paper 7) (hereinafter, "*Toyota Motor Corp.*").

[13] *See Conopco, Inc. v. Proctor & Gamble Co.*, Case IPR2014-00628, slip op. at 11 (PTAB October 20, 2014) (Paper 21) (discouraging filing of a first petition that holds back prior art for use in later attacks against the same patent if the first petition is denied); *Toyota Motor Corp.*, slip op. at 8 ("[T]he opportunity to read Patent Owner's Preliminary Response in IPR2015-00634, prior to filing the Petition here, is unjust.").

7. the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

See also LG Elecs. Inc. v. Core Wireless Licensing S.A.R.L., Case IPR2016-00986 (PTAB Aug. 22, 2016) (Paper 12) (hereinafter, "*LG Electronics*").

Applying these factors to the follow-on petitions, we concluded that the circumstances did not warrant institution of *inter partes* reviews. *See* Dec. 11–12. For instance, when evaluating factor 1, we noted that the same claims of the same patent were at issue in the follow-on petitions as in the first-filed petitions, where institutions were denied. *See id.* at 7–8. We also considered the timing of the filings under factors 2 and 3. The follow-on petitions were all filed nine months after the filing of the first-filed petitions. At the time Petitioner filed the follow-on petitions, Patent Owner had filed its Preliminary Responses to the first-filed petitions, and the Board had issued Decisions Denying Institution of the first-filed petitions, as well as Decisions Denying Rehearing of those decisions. *Id.* at 10–12. Petitioner provided no meaningful explanation for the delay in filing the follow-on petitions. Instead, Petitioner stated that it had found new prior art as a result of two later searches. *Id.* at 8. The new prior art searches did not commence until after the Board issued the Decisions Denying Institution in the proceedings based on the first-filed petitions. *Id.* at 8–9 (citing Ex. 1010 ¶¶ 3, 4, 6–8). Additionally, with respect to factor 6, we found that the Board's resources would be more fairly expended on initial petitions, rather than follow-on petitions. Dec. IPR2016-01360, 9.

With respect to factors 4 and 5, Petitioner provided no explanation in its Petition or in its Reply to Patent Owner's Preliminary Response of any unexpected

circumstances that prompted the new prior art searches, or for the delay. Dec. 11. Petitioner demonstrated that it found new prior art, but provided no explanation why it could not have found this new prior art earlier—prior to filing the first-filed petitions—through the exercise of reasonable diligence. *Id.*

We additionally found that Petitioner had modified its challenges in the follow-on petitions in an attempt to cure the deficiencies that the Board identified in its first-filed petitions. *See, e.g.*, Dec. 11–12 ("The shift in the prior art asserted and arguments in serial proceedings is of particular concern here."). More specifically, the newly-asserted prior art, predominantly directed to toner cartridges only, "without resort to any copier components as part of its invalidity arguments," was a shift in Petitioner's positions and arguments from the first-filed petitions based on the analysis articulated in our Decisions Denying Institution of those petitions. *Id.* at 12. Moreover, the shift in Petitioner's challenges was not the consequence of a position that Patent Owner surprisingly advanced or the Board surprisingly adopted, because "[t]he claims clearly require the sealing member to be a component of the toner supply container, e.g., a toner cartridge," and not the copier itself. Dec. IPR2016-01360, 9. On these bases, we stated that "[t]he filing of sequential attacks against the same claims, with the opportunity to morph positions along the way, imposes inequities on [Patent Owner]." *See* Dec. 12.

In light of the circumstances of these cases, and our assessment that the factors strongly favored non-institution, we exercised discretion and denied institution under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a). *See id.*

3. Petitioner's Contentions

Petitioner asserts that we were "overly concerned with the perceived burdens that would be imposed on the Patent Office and Patent Owner . . . , but ignored the overarching purpose of Section 6 of the America Invents Act ('AIA'), 35 U.S.C. § 311 et seq., which is to improve the quality of patents by cancelling unpatentable claims." Req. Reh'g 2. More specifically, Petitioner asserts that, in rendering our Decisions Denying Institution, our actions were contrary to the legislative purpose of 35 U.S.C. § 314(a) and that we misapplied the factors set forth in *NVIDIA*, thereby creating an improper *de facto* bar against all follow-on petitions filed after a decision on a first-filed petition. *Id.* at 1–3, 6–14.

Petitioner argues that it is not limited explicitly to filing just one petition per challenged patent under either 35 U.S.C. §§ 311 or 314, and that 35 U.S.C § 325(d) recognizes the possibility of subsequent petitions. Req. Reh'g 5–6. Petitioner further argues that § 325(d) only allows us to reject follow-on petitions when "the same or substantially the same prior art or arguments previously were presented to the Office" in the first-filed petition. *Id.* Petitioner asserts that utilizing § 314(a) and factors to prohibit shifting positions or arguments "conflicts with the express wording of § 325(d)," renders that statutory section superfluous or meaningless, and represents an abuse of discretion. *Id.* at 14.

Petitioner contends that the more specific statutory section addressing multiple proceedings (i.e., § 325(d)) controls over the more general statutory section (i.e., § 314(a)). Req. Reh'g 14 (referring to *HCSC-Laundry v. United States*, 450 U.S. 1, 6 (1981)). Petitioner asserts that, upon reviewing the legislative history, the intent of Congress in giving the Director discretion to deny petitions

under § 314 is limited to providing a "safety valve" for situations where the one-year deadline imposed by 35 U.S.C. § 316(a)(11) could not be met. *Id.* at 6–7 (citing *A Guide to the Legislative History of the America Invents Act: Part II of II*, 21 Fed. Cir. B.J. 539, 610 (2012) (citing 157 CONG. REC. S1377 (daily ed. Mar. 8, 2011))). Petitioner then argues that we should give more weight to factor 7, i.e., the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review, than to the other factors we consider because that factor is the only factor "supported by the legislative history of §314(a)." *Id.* at 7. Petitioner further argues that we did not deny institution of the follow-on petitions in order to alleviate an existing backlog of instituted proceedings affecting the Board's ability to meet a one-year deadline under § 316(a)(1). *Id.*

Petitioner also argues that § 314(a) should not be applied here because its application "improperly conflicts with 35 U.S.C. § 325(d)." *Id.* at 13. According to Petitioner, the Board previously has applied "just § 325(d)" to determine whether institution should be granted for subsequent petitions. *Id.* at 13–14 (citing *Microsoft Corp. v. Bradium Techs. LLC*, Case IPR2016-00449, slip op. at 6–10 (PTAB July 27, 2016) (Paper 9) (hereinafter, "*Microsoft*"); *Atlas Copco Airpower N.V. v. Kaeser Kompressoren SE*, Case IPR2015-01421, slip op. at 6–8 (PTAB Dec. 28, 2015) (Paper 8) (hereinafter, "*Atlas*")).

Petitioner further questions our findings on the reasonableness of its initial prior art search and argues that we abused our discretion because, under factor 2, we applied a standard based on whether the new prior art discovered by Petitioner "should have been known" earlier. Req. Reh'g 7–8. Petitioner argues that our

interpretation of factor 2 "would be self-defining to be adverse to Petitioners in every instance." *Id.* at 8. Petitioner argues that because a petition requesting an *inter partes* review can be based only on "prior art consisting of patents or printed publications," that "a reference must be locatable by a reasonably diligent search" "in order to qualify as such prior art." *Id.* As a consequence, Petitioner asserts that any prior art citable in a second petition "necessarily could have been found by a reasonable prior art search performed prior to filing the first petition." *Id.* (citing 35 U.S.C. § 311(b); *In re Lister*, 583 F.3d 1307, 1311–12 (Fed. Cir. 2009)).

Petitioner also argues that denial of a first-filed petition "should not be fatal." Req. Reh'g 10. Petitioner argues we should not have denied its follow-on petitions that attempt to cure "a substantive and material defect" in its first-filed petitions, because that rationale "would apply to any second petition filed after the Board's denial of the first petition." Req. Reh'g 10–11. To illustrate this point, Petitioner refers to two other cases where the Board instituted an *inter partes* review on grounds asserted in follow-on petitions, even though the petitioners shifted positions in the follow-on petitions. *Id.* at 10–11 (citing *Atlas*, slip op. at 6, 19; *Microsoft*, slip op. at 6–10). Petitioner further alleges that denial of the first-filed petitions was "surprising" to it because of our interpretation of "toner supply container," that distinguished the prior art presented in the first-filed petitions—which disclosed a "combination copier-toner cartridge." *Id.* at 11.

Finally, Petitioner alleges that we erred in taking the "perceived unfair prejudice" to Patent Owner into account in our denial of the follow-on petitions because the *NVIDIA* decision does not include a factor addressing Patent Owner's resources. *Id.* at 13. Instead, similar to its other arguments, Petitioner asserts that

any prejudice to Patent Owner is addressed by § 325(d), and that Patent Owner has not—and cannot show—that the follow-on petitions include the same or substantially the same prior art or arguments as the first-filed petitions. *Id.*

4. Discussion

For the reasons discussed below, Petitioner has not shown that our Decisions Denying Institution of *inter partes* review misapprehended or overlooked any matter or that we abused our discretion in reaching this determination.

i. Applying Factors to Evaluate the Equities of Permitting Follow-on Petitions is a Proper Exercise of Discretion Under 35 U.S.C. § 314(a)

The Director has discretion to institute an *inter partes* review under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a). *See* 35 U.S.C. § 314(a) (stating "[t]he Director *may not* authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition" (emphasis added)); 37 C.F.R. § 42.108(a) (stating "the Board *may* authorize the review to proceed on all or some of the challenged claims and on all or some of the grounds of unpatentability asserted for each claim" (emphasis added)). There is no *per se* rule precluding the filing of follow-on petitions after the Board's denial of one or more first-filed petitions on the same patent. The Board consistently has considered a number of factors in determining whether to exercise that discretion. *See NVIDIA*, slip op. at 6–8; *LG Electronics* at 6–7; *see also Xactware Sols., Inc. v. Eagle View Techs.,*

Inc., Case IPR2017-00034, slip op. at 7–8 (PTAB Apr. 13, 2017) (Paper 9). To reiterate, those factors are as follows:

1. whether the same petitioner previously filed a petition directed to the same claims of the same patent;
2. whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;
3. whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition;
4. the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;
5. whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;
6. the finite resources of the Board; and
7. the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

See NVIDIA, slip. op. at 6–7. Such a non-exhaustive list of factors informs practitioners and the public of the Board's considerations in evaluating follow-on petitions.

In exercising discretion under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a), we are mindful of the goals of the AIA—namely, to improve patent quality and make the patent system more efficient by the use of post-grant review procedures. *See* H.R. Rep. No. 112-98, pt. 1, at 40 (2011). Although we recognize that an objective of the AIA is to provide an effective and efficient alternative to district

court litigation, we also recognize the potential for abuse of the review process by repeated attacks on patents. *See id.* at 48 ("While this amendment is intended to remove current disincentives to current administrative processes, the changes made by it are not to be used as tools for harassment or a means to prevent market entry through repeated litigation and administrative attacks on the validity of a patent. Doing so would frustrate the purpose of the section as providing quick and cost effective alternatives to litigation.").

Our intent in formulating the factors was to take undue inequities and prejudices to Patent Owner into account. Thus, factor 3 is directed to Petitioner's potential benefit from receiving and having the opportunity to study Patent Owner's Preliminary Response, as well as our institution decisions on the first-filed petitions, prior to its filing of follow-on petitions. As discussed in our Decisions Denying Institution, we are concerned here by the shifts in the prior art asserted and the related arguments in follow-on petitions. *See* Dec. 11. Multiple, staggered petitions challenging the same patent and same claims raise the potential for abuse. The absence of any restrictions on follow-on petitions would allow petitioners the opportunity to strategically stage their prior art and arguments in multiple petitions, using our decisions as a roadmap, until a ground is found that results in the grant of review.[14] All other factors aside, this is unfair to patent

[14] The Board has addressed efficiency and potential prejudice induced by multiple petitions in multiple cases. *See LG Electronics*, slip op. at 12 ("The Board's resources would be more fairly expended on first petitions rather than on a follow-on petition like the Petition in this case."); *Butamax Advanced Biofuels LLC v. Gevo*, Case IPR2014-00581, slip op. at 12–13 (PTAB Oct. 14, 2014) (Paper 8) ("[T]he four obviousness grounds are 'second bites at the apple,' which use our prior decision as a roadmap to remedy Butamax's prior, deficient challenge.

owners and is an inefficient use of the *inter partes* review process and other post-grant review processes. Considering other factors (i.e., factors 2, 4, and 5) allows us to assess and weigh whether a petitioner should have or could have raised the new challenges earlier.

We recognize that there may be circumstances where multiple petitions by the same petitioner against the same claims of a patent should be permitted, and that such a determination is dependent on the facts at issue in the case. The factors set forth above, in our view, represent a formulation of relevant considerations that permit the Board to assess the potential impacts on both the efficiency of the *inter partes* review process and the fundamental fairness of the process for all parties. We recognize, also, that additional factors may arise in other cases for consideration, where appropriate. However, the factors set forth above, at the very least, serve to act as a baseline of factors to be considered in our future evaluation of follow-on petitions.

As we discussed above, § 314(a) recites "may not" when referring to authorization for *inter partes* review, and does not specify any particular

---

Allowing similar, serial challenges to the same patent, by the same petitioner, risks harassment of patent owners and frustration of Congress's intent in enacting the Leahy-Smith America Invents Act. *See* H.R. Rep. No. 112-98, pt.1, at 48 (2011)."); *Conopco*, slip op. at 5 ("We are not persuaded that we erred by adopting a more flexible approach that assesses each case on its particular facts to achieve a result that promotes the efficient and economical use of Board and party resources, and reduces the opportunity for abuse of the process."); *Travelocity.com L.P. v. Cronos Tech., LLC*, Case CBM2015-00047, slip op. at 13 (PTAB June 15, 2015) (Paper 7) ("Moreover, a decision on a petition . . . is not simply part of a feedback loop by which a petitioner may perfect its challenges through a subsequent filing.").

circumstance in which review must be authorized. That means institution of review is committed to the Director's discretion, which, in turn, has been delegated to the Board. *See* 35 U.S.C. § 314(a); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2140 (2016); 37 C.F.R. § 42.4(a). Similarly, under § 325(d), whether "the same or substantially the same prior art or arguments previously were presented to the Office" is an issue that "may" be taken into account in considering institution, also manifesting the discretionary nature of application of § 325(d). As such, § 325(d) is not intended to be the sole factor in the exercise of discretion under § 314(a). We, therefore, do not agree with Petitioner that our Decisions Denying Institution conflict with the "express wording" of § 325(d), or render the aforementioned provision superfluous or meaningless. We also do not agree that the legislative history indicates an intent to limit discretion under § 314(a), such that it is subordinate to or encompassed by § 325(d). Additionally, although the legislative history reflects recognition of a desire for a "safety valve" to alleviate backlog, it does not limit the exercise of discretion under 35 U.S.C. § 314(a) to only circumstances in which there is a high volume of pending proceedings. *See* 157 CONG. REC. S1377 (Mar. 8, 2011). In any event, no such restriction appears in the language of 35 U.S.C. § 314(a), and we decline to read into 35 U.S.C. § 314(a) such a restriction.

ii. Applying the Factors in These Cases

As summarized above, *supra* Section II.B.2, we find that, in these cases, six of the seven factors weigh against institution. Petitioner disputes our findings on the issue of whether Petitioner "should have known" of the art asserted in the follow-on petitions under factor 2. We disagree with Petitioner's characterization

that invariably factor 2 could not be met because "patents or printed publications" necessarily "must be locatable by a reasonably diligent search." Req. Reh'g 8. The relevant issue under factor 2 is not, as Petitioner has framed it, whether the prior art references relied on in the follow-on petitions constitute printed publications, but whether they could have been found with reasonable diligence. Thus, even for printed publications, a petitioner is free to explain why a reasonably diligent search could not have uncovered the newly applied prior art. *See Apotex Inc. v. Wyeth LLC*, IPR2015-00873, slip op. at 6 (Sept. 16, 2015) (Paper 8) (describing "[w]hat a petitioner 'could have raised,'" as including "prior art which a skilled searcher conducting a diligent search reasonably could have been expected to discover."). Here, the record is devoid of any explanation why Petitioner could not have found the newly asserted prior art in any earlier search(es) through the exercise of reasonable diligence.

In the Replies to Patent Owner's Preliminary Responses, Petitioner did not argue that there were any changed circumstances that reasonably justified its new prior art searches and associated filing of follow-on petitions. *See* Reply 1–5. In the Requests for Rehearing, however, Petitioner avers that denial of the first-filed petitions was "surprising" to it, because the Board treated the term "toner supply container" in the claim preamble as limiting. Req. Reh'g 10–11. We determine that the "surprising" argument is not entitled to consideration, because it was not included in the Replies, which we authorized in order to allow Petitioner to address Patent Owner's Preliminary Responses that raised the issues of impropriety of follow-on petitions and application of discretion under § 314(a).

In any event, Petitioner's assertion that it was "surprised" by our claim construction is unpersuasive, because that is not the pertinent issue. Rather, any such inquiry is directed to whether, from an objective perspective in the context of the applicable law and facts, Petitioner's alleged surprise is reasonable. Here, we determine that it is not. As we found, although the term "toner supply container" is in the claim preamble, it is the stated specific structure of the claim. *See* Dec. IPR2016-01360, 9. As such, it is a structural limitation appearing in the claim, and Petitioner's assertion of being surprised by our giving weight to the term is not reasonable. Furthermore, there are additional deficiencies in the first-filed petitions, identified and discussed in our denial of those first-filed petitions, which are not related to whether all claim elements have to be components of a toner supply container.

As discussed above, multiple, staggered petition filings, such as those here, are an inefficient use of the *inter partes* review process and the Board's resources. Additionally, although Petitioner contends that institution was granted in other non-precedential Board decisions alleged to be similar, we do not find that argument availing. Each case is decided on the basis of its own facts, and the Board's consideration of the factors we set forth above may vary from case to case. Finally, Petitioner's argument on the absence of specific findings on a need to alleviate an existing backlog of instituted *inter partes* reviews at the Board (Req. Reh'g 7) is not convincing. For the reasons discussed above, Petitioner's arguments on this issue are not persuasive.

Therefore, we conclude that we did not misapprehend or overlook any issues in our analysis and evaluation associated with denying institution of the follow-on petitions at issue.

III. CONCLUSION

For the foregoing reasons, Petitioner has not demonstrated that we abused our discretion, or that we misapprehended or overlooked any issue, in denying institution of *inter partes* reviews in Cases IPR2016-01357, IPR2016-01358, IPR2016-01359, IPR2016-01360, and IPR2016-01361.

IV. ORDER

Accordingly, it is ORDERED that the request for an expanded panel is *granted* and, in all other respects, Petitioner's Requests for Rehearing in Cases IPR2016-01357, IPR2016-01358, IPR2016-01359, IPR2016-01360, and IPR2016-01361 are *denied*.

IPR2016-01357 (Patent 9,046,820 B1)
IPR2016-01358 (Patent 9,046,820 B1)
IPR2016-01359 (Patent 8,909,094 B2)
IPR2016-01360 (Patent 8,909,094 B2)
IPR2016-01361 (Patent 8,909,094 B2)

For PETITIONER:

Steven F. Meyer
Tim Tingkang Xia
LOCKE LORD LLP
smeyer@lockelord.com
txia@lockelord.com

For PATENT OWNER:

Edmund J. Haughey
Michael Sandonato
Justin J. Oliver
FITZPATRICK, CELLA, HARPER & SCINTO
canon820ipr@fchs.com

Trials@uspto.gov
571-272-7822

Paper 10
Entered: December 13, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ONE WORLD TECHNOLOGIES, INC. d/b/a TECHTRONIC INDUSTRIES POWER EQUIPMENT,
Petitioner,

v.

THE CHAMBERLAIN GROUP, INC.,
Patent Owner.

Case IPR2017-01546
Patent 7,224,275 B2

Before JONI Y. CHANG, JUSTIN T. ARBES, and JON M. JURGOVAN, *Administrative Patent Judges.*

JURGOVAN, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Petitioner, OneWorld Technologies, Inc. d/b/a Techtronic Industries Power Equipment, filed a Petition requesting an *inter partes* review of claims 1, 4–6, 9–11, 14, 15, 21, 22, and 24–28 of U.S. Patent No. 7,224,275 B2 (Ex. 1001, "the '275 patent"). Paper 2 ("Pet."). Patent Owner, The Chamberlain Group, Inc., filed a Preliminary Response. Paper 6 ("Prelim. Resp."). Pursuant to our authorization, Petitioner filed a Reply and Patent Owner filed a Sur-Reply. *See* Papers 7–9.

Upon consideration of the Petition, Preliminary Response, Reply, and Sur-Reply, we exercise our discretion to deny institution of trial on this Petition under 35 U.S.C. § 314(a). Therefore, we do not institute an *inter partes* review as to the challenged claims of the '275 patent.

A. Related Matters

Petitioner indicates the '275 patent is asserted against Petitioner in *Chamberlain Group, Inc. v. Techtronic Industries Co.*, No. 16-cv-06097 (N.D. Ill. filed June 10, 2016). Pet. 1. Petitioner also identifies other patents that Patent Owner is presently asserting against Petitioner in various proceedings: U.S. Patent No. 7,635,966 B2 is involved in *Chamberlain Group, Inc. v. Techtronic Industries Co.*, No. 16-cv-06097 (N.D. Ill. filed June 10, 2016), and U.S. Patent Nos. 7,339,336 B2, 7,161,319 B2, and 7,196,611 B2 are involved in *Chamberlain Group, Inc. v. Techtronic Industries Co.*, No. 16-cv-06094 (N.D. Ill. filed June 10, 2016) and *Certain Access Control Systems and Components Thereof*, ITC Investigation No. 337-TA-1016 (instituted Aug. 3, 2016). Pet. 1–2. Petitioner previously filed other petitions seeking *inter partes* review of claims of the '275 patent (Cases IPR2016-01772 (claims 1–6, 9–12, and 14–23) (institution denied) and IPR2016-01774 (claims 24–31) (institution denied)).

Petitioner also has filed petitions against the following patents: U.S. Patent No. 6,998,977 B2 (Cases IPR2017-01132 (trial instituted) and IPR2016-01137 (trial instituted)); U.S. Patent No. 7,635,966 B2 (Cases IPR2016-01846 (institution denied), IPR2017-01040 (institution denied), and IPR2017-01042 (institution denied)); U.S. Patent No. 7,171,319 B2 (Case IPR2017-00126 (trial instituted)); U.S. Patent No. 7,196,611 B2 (Cases IPR2017-00073 (trial instituted) and IPR2017-00214 (trial instituted)); and U.S. Patent No. 7,339,336 B2 (Case IPR2017-00432 (institution denied)).

B. Illustrative Claim

Of the challenged claims, claims 1, 14, and 24 are independent. Claim 1 is illustrative:

> 1. A movable barrier operator comprising:
> a controller having a plurality of potential operational status conditions defined, at least in part, by a plurality of operating states;
> a movable barrier interface that is operably coupled to the controller;
> a wireless status condition data transmitter that is operably coupled to the controller, wherein the wireless status condition data transmitter transmits a status condition signal that:
> corresponds to a present operational status condition defined, at least in part, by at least two operating states from the plurality of operating states; and
> comprises an identifier that is at least relatively unique to the movable barrier operator, such that the status condition signal substantially uniquely identifies the movable barrier operator.

Ex. 1001, 8:5–21.

C. Prior Art Relied Upon

Petitioner relies upon the following prior art reference:

Kikuya JP 2001-349141A Dec. 21, 2001

Ex. 1003 (Japanese version); Ex. 1004 (certified English translation).

D. Asserted Grounds of Unpatentability

Petitioner asserts the following ground of unpatentability:

Challenged Claims	Basis	Reference
1, 4–6, 9–11, 14, 15, 21, 22, and 24–28	§ 102(b)[1]	Kikuya

Pet. 1–3.

II. ANALYSIS

35 U.S.C. § 314(a) provides as follows:

> **§ 314. Institution of inter partes review**
> **(a).Threshold.**—The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

This section grants the Board discretion to deny institution of a later-filed petition based on various factors, as set forth in *General Plastic Indus. Co. v. Canon Kabushiki Kaisha*, Case IPR2016–01357, slip op. 15–19 (PTAB September 6,

[1] Because the claims at issue have an effective filing date prior to March 16, 2013, the effective date of the applicable provisions of the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), we apply the pre-AIA version of 35 U.S.C. § 102 in this Decision.

2017) (Paper 19) ("*General Plastic*") (Section II.B.4.i designated as precedential[2]) (citing *NVIDIA Corp. v. Samsung Elec. Co.*, IPR2016-00134, slip op. 6–7 (PTAB May 4, 2016) (Paper 9)). The non-exhaustive factors are as follows:

1. whether the same petitioner previously filed a petition directed to the same claims of the same patent;

2. whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;

3. whether at the time of filing of the second petition the petitioner already received the patent owner's preliminary response to the first petition or received the Board's decision on whether to institute review in the first petition;

4. the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;

5. whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;

6. the finite resources of the Board; and

7. the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

We address each of these factors in turn, but note that not all the factors need to weigh against institution for us to exercise our discretion under § 314(a).

[2] Section II.B.4.i of *General Plastic* was designated precedential on October 18, 2017. The decision previously had been designated informative on September 18, 2017.

1. First Factor: Whether the Petitions are Directed to the Same Claims

Concerning factor (1) in relation to the facts of this case, the Petition was filed on June 12, 2017, and challenges claims 1, 4–6, 9–11, 14, 15, 21, 22, and 24–28 of the '275 patent. Previously, on September 9, 2016, Petitioner filed a petition in Case IPR2016-01772 challenging claims 1–6, 9–12, and 14–23 and a petition in Case IPR2016-01774 challenging claims 24–31 of the '275 patent. Thus, all of the claims challenged in this Petition were challenged in the previous petitions. Consequently, this factor weighs against institution.

2. Second Factor: Whether Petitioner Knew or Should Have Known of the Newly Asserted Prior Art

Considering factor (2), Petitioner states that on January 25, 2017, the Court of Appeals for the Federal Circuit ("Federal Circuit") vacated the claim construction of the District Court of the Northern District of Illinois ("District Court"), holding that the "controller" recited in the claims of the '275 patent may rely upon external sensors to obtain status conditions. Pet. 6. Petitioner states the Federal Circuit's construction prompted Petitioner to engage a new search firm on February 23, 2017, which located the Kikuya reference and provided it to Petitioner on April 12, 2017. *Id.* at 7. Upon review, Petitioner states it identified the Kikuya reference as anticipatory prior art and filed the present Petition. *Id.*

The relevant question under factor (2), however, is whether Petitioner knew or should have known of the Kikuya reference at the time of filing its first two petitions (September 9, 2016). Petitioner does not provide any explanation as to why the reference could not have been found with a reasonably diligent search at the time of the earlier petitions. *See General Plastic* at 11 ("Petitioner . . . provided no explanation why it could not have found this new prior art earlier—prior to filing the first-filed petitions—through the exercise of reasonable

diligence."), 19 ("the record is devoid of any explanation why Petitioner could not have found the newly asserted prior art in any earlier search(es) through the exercise of reasonable diligence").

Furthermore, what bearing the Federal Circuit's claim construction (or those of the Board or the District Court) had on whether the Kikuya reference reasonably could have been located earlier is not explained adequately in the Petition. In this regard, we note that Petitioner states that it requested the later patent search on February 23, 2017, which was shortly after receiving our decisions denying institution in Cases IPR2016-01772 and IPR2016-01774 on February 21, 2017. Petitioner makes no mention of how this factored into the decision to request the later patent search.

Moreover, Petitioner states that it requested the patent search that yielded the Kikuya reference on February 23, 2017, and the District Court adopted a "broader construction" in an order issued April 7, 2017. Pet. 7. Given this sequence of events, we do not see how the scope of the patent search could have taken into account a "broader" claim construction that did not exist when Petitioner requested the later patent search. We agree with Patent Owner that factor (2) weighs in favor of exercising our discretion to deny the Petition. *See* Prelim. Resp. 10–14.

In view of the foregoing, this factor weighs against institution.

3. *Third Factor: Whether Information from Prior Proceedings was Available*

As to factor (3), the preliminary responses in Cases IPR2016-01772 and IPR2016-01774 were filed on December 23, 2016 and December 27, 2016, respectively. As noted, our decisions denying institution were entered on February 21, 2017. Thus, Petitioner had received Patent Owner's preliminary responses and our decisions on institution in Cases IPR2016-01772 and IPR2016-01774 before

filing the present Petition, and thus had the advantage of knowing what was in them in preparing the present Petition.

Consequently, this factor weighs against institution.

4. Fourth Factor: Elapsed Time

Concerning factor (4), Petitioner states that it received the Kikuya reference on April 12, 2017, and filed the Petition two months later on June 12, 2017. Pet. 7. Petitioner suggests time was needed to identify and review the Kikuya reference and prepare the Petition. *Id.* However, although a period of two months may be reasonable, Petitioner does not explain why two months was a reasonable time under the circumstances in which to file the Petition.

Accordingly, this factor neither weighs for or against institution.

5. Fifth Factor: Whether Petitioner Provides Adequate Explanation

Regarding factor (5), Petitioner states it conducted "a more than reasonably diligent prior art search in 2016 using a top prior art search firm." *Id.* at 8. Petitioner also states that the ground asserted in this Petition "is not similar to any of the prior art relied upon in the earlier petitions, and the new art was not located despite a diligent search." *Id.* at 10. However, these statements are conclusory, and do not provide sufficient detail to justify the nine months that elapsed between filing the petitions in Cases IPR2016-01772 and IPR2016-01774, and the present Petition, directed to the '275 patent. Also, we are not persuaded that any changed claim construction was unexpected or surprising to Petitioner. *See General Plastic* at 11 ("the shift in Petitioner's challenges was not the consequence of a position that Patent Owner surprisingly advanced or the Board surprisingly adopted").

Other considerations that have a bearing on factor (5) were discussed previously (see particularly the discussion under factor (2)).

For these reasons, this factor weighs against institution.

6. Sixth and Seventh Factors: Board Resources and Final Determination

As to factors (6) and (7), analysis of "multiple, staggered petition filings" is, in general, "an inefficient use of the *inter partes* review process and the Board's resources." *General Plastic*, slip op 21. Board resources are more fairly expended on initial petitions rather than follow-on petitions. *See id.* at 10. In short, the finite resources of the Board weigh against institution in this case.

Conclusion

For the reasons discussed above, we determine a majority of the *General Plastic* factors weigh strongly against institution in this case. Accordingly, we exercise our discretion to deny institution under 35 U.S.C. § 314(a) and 37 C.F.R. § 42.108(a).

III. ORDER

For the foregoing reasons, it is

ORDERED that the Petition is denied as to all challenged claims of the '275 patent.

For PETITIONER:

Dion Bregman
Jason C. White
Michael Lyons
Ahren C. Hsu-Hoffman
MORGAN, LEWIS & BOCKIUS LLP
Jason.white@morganlewis.com
Dion.bregman@morganlewis.com
Ahren.hsu-hoffman@morganlewis.com
michael.lyons@morganlewis.com

For PATENT OWNER:

W. Karl Renner
Joshua Griswold
Jeremy J. Monaldo
Dan Smith
FISH & RICHARDSON P.C.
axf-ptab@fr.com
griswold@fr.com
jjm@fr.com
dsmith@fr.com

Exhibit A

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

PROXENSE, LLC, Plaintiff, vs. SAMSUNG ELECTRONICS, CO., LTD. AND SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Case Nos. 6:21-cv-00210-ADA **JURY TRIAL DEMANDED**

DECLARATION OF DR. SETH JAMES NIELSON IN SUPPORT OF SAMSUNG'S OPENING CLAIM CONSTRUCTION BRIEF

I, Seth James Nielson, declare as follows:

1. I am qualified and authorized to attest to the matters set forth in this Declaration. I have knowledge of the facts set forth in this Declaration based on my own personal information or investigation into the relevant subject matter.

I. INTRODUCTION

2. I am over the age of 18 and am competent to make this Declaration. I have personal knowledge or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

3. I have been retained by counsel for defendants Samsung Electronics, Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") as an expert to provide opinions regarding the understanding of a person of ordinary skill in the art ("POSITA") in connection with certain terms in the claims of U.S. Patent Nos. 8,352,730 (the "'730 patent"), 9,049,188 (the "'188 patent"), 9,235,700 (the "'700 patent"), 9,298,905 (the "'905 patent"), and 10,698,989 (the "'989 patent") (collectively, "Patents-in-Suit").

4. I am being compensated at my usual hourly rate of $600 per hour. I am also being reimbursed for any out-of-pocket expenses. I have no financial interest in, or affiliation with, Samsung. My compensation does not depend in any way on the outcome of this case, the substance of my testimony, or opinions that I express.

5. In rendering my opinions, I have considered the patents at issue, their file histories, the parties' claim construction disclosures, and any other documents referenced, discussed, or listed in my declaration, and my own knowledge and experience in the user interface, computer networking, wireless communications, telecommunications networks, relational database

management system, data structures, algorithms, and other computing fields relevant to the asserted patents.

6. In forming my opinions, I understand that the claims should be interpreted as they would be understood by a POSITA of the patent at the time its application was filed. I understand that the claims are to be construed with reference to the patent's specification, the claims, the prosecution history, in light of the plain meaning of the terms used in the claims, and with potential reference to other sources of information, such as dictionaries, textbooks, and literature or other patents in the same or related fields.

7. My analysis of the materials produced in this matter is ongoing and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to amend or supplement my opinions based on additional documents or evidence I am presented, including without limitation any arguments or expert declarations advanced by either party in this case.

I. QUALIFICATIONS AND EXPERIENCE

8. My qualifications are summarized below and are addressed more fully in my CV attached as Exhibit A to this declaration.

9. I am a subject matter expert in cyber security, including the sub-fields of applied cryptography and network security. I am the Founder and Chief Scientist of Crimson Vista, a computer security research and engineering company. Furthermore, I hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the Department of Computer Science and as a Cybersecurity Fellow in the Robert Strauss Center for International Security and Law.

10. I have been working professionally in the field of computer security since August of 2005 and within the field of computer science generally since June 2000. My experience

includes graduate-level teaching, academic research, industry employment, and consulting practice.

11. I received my B.S. in Computer Science in April of 2000. During my final undergraduate semester, I worked both as a teaching assistant for a Computer Networking course and as a researcher in the Networked Computing Lab. In these capacities, I assisted students in debugging and designing TCP/IP protocol stacks, Address Resolution Protocol implementations, and Remote Procedure Call projects. I have collaborated on investigations of statistical traffic engineering for bandwidth allocation, including a published paper entitled, "Effective Bandwidth for Traffic Engineering."

12. After graduation (from 2001 through 2003), I worked as a software engineer at Metrowerks (formerly Lineo, Inc.), where I had substantial responsibilities relating to software architecture, computer networking, and technical project management.

13. As part of my technical training and development at Lineo/Metrowerks, I also gained and employed a wide exposure to computer networking and an introduction to network security. I tested and evaluated a prototype firewall product, built a custom VPN solution, and trained in the use of web server and mail server administration. I ran my own personal MTA with an IMAP and POP3 server based on these tools under development.

14. Another major networking project involved porting the Embedix SDK from Linux to Windows. For this project I used a virtual-machine/networked solution. The underlying SDK engine remained running in a Linux VM while the GUI operated in native Windows. I developed all of the code for this remote communication system.

15. Additionally, the SDK provided extensibility through a scripting system based on Python. A critical task was to make the existing Python scripts, built to run in Linux, work

unmodified with the new Windows system. I engineered a framework that automatically intercepted certain Python commands and sent them across the network to the other side, similar to RPC technology. From the perspective of the scripts, all of the function calls were local when, in fact, certain operations were executed remotely.

16. While working at Lineo/Metrowerks, I also returned to BYU to pursue my Master's degree in Computer Science. In addition to the graduate level course work in wireless computer networks and compilers, I pursued graduate research in software engineering topics, with a special emphasis on how programmers think while creating and modifying code. My research included a study of computer architectural patterns and how those patterns might need to change as programming languages change and evolve. Based on my research, I proposed a concept called "Design Dysphasia," wherein a programmer or software developer becomes trapped in their approach to solving problems based on the paradigms and design approaches of the programming language. My research was published as "Design dysphasia and the pattern maintenance cycle," in the Journal Information and Software Technology August 2006. This work also was a major component of my Master's thesis.

17. After finishing my Master's degree, I moved to Houston TX in 2004 to begin a PhD program at Rice University. At this point, my interest in computer security took priority over my interests in programming languages and software engineering, and my classes and research were directed to that topic.

18. During the 2004 fall semester of my Ph.D. program at Rice University, I identified a security vulnerability in the Google Desktop Search that could have allowed hackers to compromise users' computers and obtain private information. After contacting Google and assisting them in closing the vulnerability, we published the details of our investigation.

19. In 2005, I completed an internship at Google, where I designed and implemented a solution to privacy loss in Google Web Accelerator. The Google Web Accelerator was designed to increase the speed of browsing the Internet. Once installed on a user's computer, the browser would request all content through a Google Proxy. The proxy performed pre-fetching and extensive caching in order to provide fast and responsive service to the user. At the time of my internship, news reports had identified odd problems in which users of the Accelerator were accessing other individual's private pages. During my internship, I designed and implemented a prototype solution for this issue in C++.

20. In 2005, I published a paper entitled, "A Taxonomy of Rational Attacks." This paper categorized and described the various types of attacks that one might see in a decentralized, peer-to-peer network. When there is no centralized authority, users have to cooperate to obtain service. The term "rational attacks" refers to the economic incentives to not cooperate while still exploiting the system for service.

21. My Ph.D. Thesis was entitled "Designing Incentives for Peer-to-Peer Systems," and it built on this concept. Given a network where participants cannot be forced to cooperate, the operation of said network must induce cooperation by design of the outcomes. In other words, it must be in each participant's best interest to contribute to the cooperative operation. I conducted experiments including simulated extensions to the BitTorrent peer-to-peer protocol for long-term identities and mechanisms for cooperative anonymity.

22. From 2005 through 2008, with the approval of my PhD adviser, I worked as a Security Analyst and for Independent Security Evaluators (ISE). Much of my early work was spent developing a software encryption library, including the necessary tests and procedures for

FIPS-certification. The encryption library provided advanced operations such as secure data splitting and recovery.

23. In 2009, I went to work full time for ISE as a Security Analyst and later as a Senior Security Analyst. I built a number of advanced projects including a parallel-program for massive code coverage analysis, GPU hardware-accelerated AES encryption, and encrypted file-system prototypes.

24. In addition to the software development, I also performed security evaluation services that included port-scanning analyses, security protocol analysis using formal and exploratory methods, and investigated security breaches.

25. I also designed and managed the implementation of a secure communication technology that splits trust between multiple SSL Certificate Authorities (CA), so that if one CA is compromised, the communication stream can still be safely authenticated. My work on the secure communications technology project led to the issuance of multiple patents. In total, I wrote hundreds of thousands of lines of code in C, C++, and Python, including projects where I had to implement the same functionality in two separate languages.

26. In 2011, I began work as a Research Scientist at Harbor Labs and continued with that consulting firm until fall 2015. I worked with a wide range of clients, specializing in network security, network communications, software architecture, and programming languages. I analyzed an extensive collection of commercial software, including software related to secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, and peer-to-peer communications. I also analyzed security considerations for potential technology acquisitions.

27. Also at Harbor Labs, I reviewed technology and source code for multiple clients related to accusations of theft and/or misappropriation of trade secrets. These engagements included an analysis of C, C++, Java, Python, and other source code languages in high-frequency trading, e-commerce, and other similar systems.

28. I also assessed the security and privacy technologies and policies provided by a third-party vendor to the Center for Copyright Infringement (CCI). CCI represents content owners, such as the RIAA and the MPAA, in finding and reducing piracy online.

29. For other clients, I have "resurrected" or re-created legacy software systems. For example, I assisted one client make code from the mid 90's operational. I helped them identify the most compatible components from an old CVS repository, obtain the necessary legacy hardware and software to rebuild the source code, and diagnose why the separate components weren't completely compatible with each other. Using tools from the era (*i.e.,* the mid-90's), I identified and fixed these issues in C++ and Java code, and successfully demonstrated the operational system.

30. In other similar examples, I re-created basic software in x86 Assembly code that mimicked the behavior of 1990's era viruses, wrote a file transfer system similar to FTP in pre-2.0 Java, and demonstrated the use of a command-line antivirus software adapted for router/gateway scanning.

31. During my final year at Harbor Labs, I was engaged as the principal consultant with a large biomedical device firm in a twelve-month analysis of the security of their products. Notably, medical devices were for some time not considered significant threats in terms of computer security. However, recent demonstrations by security researchers of the various ways in which a malicious individual might harm a person using a medical device has shifted the

thinking in the industry. Accordingly, I was engaged to assist this company in the analysis of their products, their process, and their future roadmap in order to ensure that patients are not harmed. My team and I analyzed design documents, hardware, and a broad range of additional resources in order to expose potential problems. The security of these systems depends, in part, on the architecture and deployment of the networks in which they operate.

32. In May 2016, I founded Crimson Vista, Inc. as a boutique computer security engineering company. Similar to the work that I did at Harbor Labs, I continue to provide technical expertise to a wide range of clients in areas of programming languages, computer networks, and network security. My expertise in the area of "security engineering" provides comprehensive analysis, design, and insight into cybersecurity concerns before, during, and after development.

33. For example, I have been retained by a start-up in telecommunications security to provide cryptography expertise and evaluations of their protocols and architectures. My team and I have prototyped new protocols, written up analyses, and presented to potential partners and investors.

34. Another start-up company retained me for guidance in matters relating to Blockchain and Smart Contracts. This technology is very much dealing with a "fad" phase where there is a lot of misinformation and hype. I guided the start-up company through where these kinds of technologies would help and where they would not. I have also provided training on Blockchain at the Data Architecture Summit and Enterprise Data World conferences.

35. I have also provided technical guidance to an antitrust team in the United States Department of Justice. Although the technologies and parties are confidential, I can disclose that I provided in-person training on technical topics and analyses of competing security products.

36. More recently, I been retained by clients, including a Fortune 100 financial institution, to provide them with post-data-breach analyses of what went wrong, the impact of the lost data, and guidance on resolution. In these engagements, I provided reverse engineering of the data to demonstrate how an attacker can or would use the compromised information, analyzed software development to determine when the system became vulnerable, and helped identify impacted customers that had been missed in the investigations.

37. Through Crimson Vista, I also invest in research and development. Recent projects include engaging with a partner to implement prototypes of communications security protocols for next-generation automobiles. I also gave a talk on "Detecting Malicious Sandboxes" at the Workshop on Defensive Deception and Trust in Autonomy, in association with the 2018 Naval Applications of Machine Learning Workshop.

38. I also continue to perform a wide range of code reviews for diverse technologies including CAD software, video game systems, digital mobile radios (DMRs), video streaming, and digital rights management (DRM).

39. Moreover, I maintain ties to academia. I have held adjunct appointments at Johns Hopkins University from 2014 to 2019. From July 2016 to July 2019 I also held an appointment as the Director of Advanced Research Projects in the Johns Hopkins University Information Security Institute.

40. At Johns Hopkins University I taught Network security and Advanced Network Security. I created a custom curriculum and lab experience wherein students develop their own security protocols as a class and then attempt to break their own creations. Students learn how hard it is to get security right, and how easy it is to find something wrong. I published a paper

about the labwork in the Journal of Computer Science Education entitled, "PLAYGROUND: Preparing Students for the Cyber Battleground."

41. The labwork in the advanced course builds on the same framework, but adds in mobile, autonomous vehicles in a game-like simulation. Students program "bots" with computer program "brains," that are used to gather resources, attack, communicate, and so forth. The students explore various opportunities for compromising the brains of the other students as part of the labs.

42. One of the components of the students' lab work is to create a protected "sandbox" for running untrusted code. The sandbox must provide access to the system in a manner that cannot be exploited. Conversely, the other half of their assignment is to design exploitative code that attempts to bypass and/or neutralize the protections of the sandbox environment. This experimental framework enables the students to learn about creating, identifying, and neutralizing malware such as viruses.

43. Beyond course instruction, I also mentored Masters students at Johns Hopkins in their capstone projects. These projects include networking security and privacy concerns across a wide range of technologies including cryptography, drone security, iOS security, BitCoin, SSL vulnerabilities, and Twitter "botnets." My students and I have published multiple papers from these capstone projects.

44. During my tenure as the Director of Advanced Research Projects, I was tasked with developing collaborative research opportunities. Through my efforts, a wide range of student capstones have been executed with partners from the Johns Hopkins Applied Physics Lab or outside corporate partners.

45. For example, we coordinated with the company OnBoard Security to develop better security for anti-collision protocols for air traffic. Students demonstrated the potential issues related to leaving the protocol unsecured and built a working prototype of a secured variant. OnBoard and Johns Hopkins published press releases which were picked up by aviation-focused news sources.

46. I am now an adjunct professor at the University of Texas at Austin. I teach the undergraduate Network Security and Privacy class in the Computer Science department. I also teach the Introduction to Cybersecurity Technology class in the Law School

47. I am also the co-founder and current director of the Crypto Done Right Foundation, a non-profit. The foundation grew out of a research project initially hosted at Johns Hopkins University and funded by a grant from Cisco. Crypto Done Right is designed to bridge the gap between cryptography SME's and the IT professionals that use it. It provides authoritative guidance on deployment, lifecycle, and management of cryptography in IT systems, software development, and technical management.

48. I am also the author of "Cryptography in Python: Learning Correct Cryptography by Example."

II. LEGAL STANDARDS

A. Claim Construction

49. I am not a lawyer, and I do not intend to offer any opinions as to the interpretation of the law. However, I have a general understanding of claim construction based on my experience with patents, my work as an expert in other cases, and my conversations with counsel.

50. I am informed that on the law regarding claim construction and patent claims, a patent may include two types of claims, independent claims and dependent claims. An

independent claim stands alone and includes only the limitations it recites. A dependent claim can depend from an independent claim.

51. I am informed that claim construction is a matter of law to be decided by the Court. I understand that claim terms are presumed to have their plain and ordinary meaning, as understood by a POSITA at the time of the invention, in the context of the patent specification, the prosecution history, and any other relevant evidence.

52. I am informed that to determine how a POSITA would understand a claim term, one should look to those sources available that show what a person of skill in the art would have understood the disputed claim language to mean. Such sources include the words of the claims themselves, the remainder of the patent's specification, the prosecution history of the patent and the cited references (all considered "intrinsic" evidence), and "extrinsic" evidence, such as dictionary definitions, learned treatises and the opinions of qualified experts concerning relevant scientific principles, the meaning of technical terms, and the state of the art.

53. I am informed that, in construing a claim term, one looks primarily to the intrinsic patent evidence, including the words of the claims themselves, the remainder of the patent specification, and the prosecution history.

54. I am informed that extrinsic evidence, which is evidence external to the patent and the prosecution history, may also be useful in interpreting patent claims when the intrinsic evidence itself is insufficient.

55. In construing claims, the claims themselves, the patent specification, and the prosecution history are of paramount importance. Additionally, the specification and prosecution history must be consulted to confirm whether the patentee has acted as its own lexicographer (*i.e.,*

provided its own special meaning to any disputed terms), or intentionally disclaimed, disavowed, or surrendered any claim scope.

56. I understand that the claims of a patent define the scope of the rights conferred by the patent. The claims must particularly point out and distinctly claim the subject matter which the patentee regards as his invention. Because the patentee is required to define precisely what he claims his invention to be, it is improper to construe claims in a manner different from the plain import of the terms used consistent with the specification. Accordingly, a claim construction analysis must begin with and remain centered on the claim language itself. Additionally, the context in which a term is used in the asserted claim can be highly instructive. Likewise, other claims of the patent in question, both asserted and unasserted, can inform the meaning of a claim term. For example, because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

57. I understand that a POSITA is deemed to read a claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. For this reason, the words of the claim must be interpreted in view of the entire specification. The specification is the primary basis for construing the claims and provides a safeguard such that correct constructions closely align with the specification. Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelope with the claim as set forth in the patent itself.

58. I understand that while intrinsic evidence is of primary importance, extrinsic evidence, *e.g.*, all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises, can also be considered. For example, technical dictionaries may help one better understand the underlying technology and the way in which one of skill in the art might use the claim terms. Extrinsic evidence should not be considered, however, divorced from the context of the intrinsic evidence. Evidence beyond the patent specification, prosecution history, and other claims in the patent should not be relied upon unless the claim language is ambiguous in light of these intrinsic sources. Moreover, while extrinsic evidence can shed useful light on the relevant art, it is less significant than the intrinsic record in determining the legally operative meaning of the claim language.

B. Indefiniteness

59. I understand that a patent must satisfy a definiteness requirement under 35 U.S.C. §112, ¶2, which requires that it conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as the invention.

60. I understand that definiteness requires that a patent's claims, viewed in light of the specification and file history from the perspective of a person skilled in the relevant art, inform those skilled in the art about the scope of the invention with reasonable certainty.

61. I understand that a patent must be precise enough to afford clear notice of what is claimed and apprise the public of what is still open to them in a manner that avoids a zone of uncertainty which enterprise and experimentation may enter only at the risk of infringement claims.

62. I understand that patents are presumed valid and indefiniteness is an invalidity defense. So, I understand that indefiniteness must be shown by clear and convincing evidence.

III. LEVEL OF ORDINARY SKILL IN THE ART

63. I understand that the claims must be understood from the perspective of a POSITA at the time of the alleged inventions. I also understand that to determine the level of skill of a POSITA, one must consider several factors including the types of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the education level of active workers in the field. I further understand that the '730, '905, and '989 patents originate from a common application and relate to substantially similar subject matter, as such the level of ordinary skill in the art of these patents would be the same. I understand this to be the same with regard to the '188 and '700 patents.

64. In my opinion, with respect to the Patents-in-Suit, a POSITA at the time of the alleged inventions would have had a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent). This level of skill is approximate, and more experience would compensate for less formal education, and vice versa.

65. I meet these criteria and consider myself a person with at least ordinary skill in the art pertaining to the asserted patents. I would have been such a person at the time of the invention of each of the asserted patents.

66. I applied this level of skill of a POSITA for purposes of my analysis in this Declaration. To my knowledge, none of Proxense's experts has yet proposed an alternative level of skill of a POSITA in this case. If and when they do, I reserve the right to provide further opinions concerning the appropriateness of that proposed level of skill of a POSITA, and to provide further opinions concerning any impact that the alternative level of skill of a person of ordinary skill would have on my analysis.

IV. PATENTS IN SUIT

67. I understand the '730 patent, the '905 patent and the '989 patent are all part of the same family, and are in the same chain of continuations, and therefore share substantially identical specifications. Furthermore, many of the claims of the '730 patent, the '905 patent and the '989 patent use the same phrases or share similar structure. Because of the substantially identical specifications and the overlap in claim language, a POSITA would interpret the claim terms of the '730 patent, the '905 patent and the '989 patent in the same context.

68. Similarly, I understand the '188 patent and the '700 patent are part of the same family, and are in the same chain of continuations, and therefore share substantially identical specifications. Furthermore, many of the claims of the '188 patent and the '700 patent use the same phrases or share similar structure. Because of the substantially identical specifications and the overlap in claim language, a POSITA would interpret the claim terms of the '188 patent and the '700 patent in the same context.

V. "THIRD PARTY TRUSTED AUTHORITY"

69. In my opinion, a POSITA would not understand the term "third party trusted authority" to be "a third component that provides a second level of authentication" according to Proxense's construction. In particular a POSITA would have understood a "third party" to not merely be a "third component." Similarly while the claim language as a whole requires that the "third party trusted authority" provide a second authentication, a POSITA would not have understood the term "third party trusted authority" itself to necessarily require "provid[ing] a second level of authentication."

70. Particularly, a POSITA reading the intrinsic evidence of the '730 Patent[1] would have understood that "third party" does not connote a party numbered after a second party. Instead,

[1] While I refer primarily to the '730 Patent, my opinion is likewise applicable to the '905 and '989 patents because they are all part of the same chain of continuations, and in my opinion, a

"third party" relates to a relationship between entities. A POSITA would have known that "third-party" is a well-understood, widely used concept in the art and especially with reference to authentication. This is consistent with the arguments presented by the '730 Patent applicant during prosecution. During prosecution, the applicant explained a "user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be" does not satisfy the "third party" limitation. Declaration of Marissa Ducca("Ducca Decl.") Ex. 4 ('730 Patent History, Applicant Arguments/Remarks Made in an Amendment (2010-02-25) at 8). The applicant emphasized the prior art "disclose[d] two parties: the user and the institution." *Id.*

71. A POSITA would further understand "third party" to relate to a specific class of entity, that of one who is not an interested party to the transaction or a witness. Again, this is the point the applicant made during prosecution. The applicant explained "sending a code to a receiver of **a door that the user is trying to access**" does not satisfy the "third party" limitation. Ducca Decl. Ex. 4 ('730 Patent History, Amendment/Req. Reconsideration – After non-Final Rejection(2010-09-07) at 8) (emphasis in the original). The door in this example is one of the two interested parties to the "access" transaction and as such would not satisfy a POSITA's understanding of "third party."

72. This reading of "third party" is similarly in accord with the specification. While the specification does not expressly mention the term "third party trusted authority" it discusses a "trusted key authority [that] is a third-party authority" which describes the claimed term. '730 Patent at 5:40-52. The specification similarly explains the "agent can be, for example, a

POSITA would understand the '905 and '989 patents in light of the '730 patent, including the '730 specification and prosecution history.

government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at 6:32-41.

73. This understanding further matches with the common use of the term "third party" in the industry, which refers typically to an entity not directly involved in the transaction. This industry definition of "trusted third party" focuses on the "third party" as an entity with a responsibility separate from executing the transaction itself: "an entity responsible for ensuring key distribution in a safe and reliable manner." Ducca Decl. Ex. 3 at 3 (Cryptographic Libraries for Developers). Third parties (and trusted third parties) are crucial elements in the field of security. For example, the use of third parties for authentication is a key part of all security courses I have taught at both Johns Hopkins University and the University of Texas at Austin.

74. Because the specification, the prosecution history, and common industry usage all suggest a "third party" refers to an entity outside of the transaction or a witness thereto rather than a "third component," it is my opinion Proxense's construction is incorrect. I have never seen Proxense's construction used in any applicable academic or industry publications or systems. It is also my opinion that Proxense's construction is technically unsound and would result in a broken authentication mechanism.

75. In my opinion the latter portion of Proxense's construction, "that provides a second level of authentication," is redundant and unnecessary. This limitation is already captured in the claim language around "third party trusted authority." In particular, the language "responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes . . . for authentication by an agent" provides that the agent provides a "second level of authentication." A POSITA would not have read this term to include a redundancy.

VI. "HYBRID DEVICE"

76. It is my opinion that the bounds of what constitutes a "hybrid device" is not clear to a POSITA in light of the patent specification and claims, and therefore the term is indefinite.

77. As an initial point, a "hybrid device" is not a term of art, and does not have an ordinary meaning in the field of encryption or security. The term "hybrid" suggests there needs to be a combination of different types or kinds of something.

78. The term "hybrid device" is described in various ways throughout the specification, but is not expressly defined anywhere.

79. Based on the intrinsic evidence, there are multiple possible different meanings for the term, of different scope and not reconcilable under a single interpretation.

80. In the abstract, a hybrid device is described as follows:

> The hybrid device operates in one of several modes including, PDK only, RDC only, or PDK and RDC. This allows a variety of system configurations for mixed operation including: PDK/RDC, RDC/RDC or PDK/PDK.

'188 Patent[2] at Abstract.

81. Based on this disclosure, it appears that a hybrid device may have multiple modes, but it is unclear if a hybrid device is required to be capable of operating in all 3 of the modes (PDK only, RDC only, or PDK and RDC) or can qualify as a hybrid device if it operates in only one or two of the listed modes.

82. The second sentence describes mixed operation, but again it is unclear whether all of the described modes (RDC/RDC, RDC/PDK, PDK/PDK) must be present and available to

[2] The '188 and '700 patent specifications are largely identical, and while the '188 patent specification is quoted throughout my declaration, identical disclosures appear in the '700 patent specification.

qualify as "mixed operation," or if operating in only one or two of the listed modes would qualify as "mixed operation."

83. It is also unclear what is meant by "mixed operation" and if, for example, RDC/RDC by itself would qualify as a "mixed operation" since it would not involve any PDK functionality. To a POSITA, perhaps a "mixed operation" would require both "RDC/RDC" and "PDK/PDK" together. Alternatively, perhaps "RDC/PDK" by itself could qualify as mixed mode. This is unclear from the disclosure above and a POSITA would not be able to determine what it means with any reasonable degree of certainty.

84. In the specification, the hybrid device is described as follows:

> The hybrid device 1102 allows for many different configurations and operations of the secure PDK/RDC protocol. The hybrid device 1102 allows mixed operations including: RDC/PDK, RDC/RDC or PDK/PDK combinations. For purposes of explanation below, each device is enabled with either or both RDC and PDK functionality.

'188 Patent at 15:64-16:2.

85. As with the disclosure in the abstract, it is unclear if "mixed operations" means all three of the listed modes, or if one or two of the modes is sufficient. As with the disclosure in the abstract, the disclosure here is also confusing because it does not describe what "mixed operations" means in this context.

86. The last sentence in the column 15 passage introduces confusion because it suggests that a device might qualify as a hybrid device with just one of (or both) RDC and PDK functionality ("either or both"). The idea that just one functionality is sufficient is counter to the ordinary meaning of "hybrid" and "mixed."

87. For the Figure 12 embodiment, the specification describes:

> While FIG. 12 shows the hybrid device 1102 as including both the RDC 304a and the PDK 102a, in another embodiment the hybrid device 1102 includes only the RDC 304a.

'188 patent at 14:20-22.

88. This passage suggests a hybrid device may consist of only the RDC. If a hybrid device consists of only a RDC, then it is not capable of mixed mode functionalities PDK/PDK and PDK/RDC, as described in the abstract and column 15. Furthermore, it cannot operate in PDK only, or PDK and RDC mode as described in the abstract and column 15.

89. Furthermore, the hybrid device is described as follows:

> the hybrid device 1102 provides authorization control as well as a storage area for storing information specific to the user.

'188 patent at 14:34-36.

90. In the claims, the PDK is consistently described as used for storing information. For example, '188 patent claim 1 states: "an integrated personal digital key (PDK) for storing local, secured biometric information." '188 patent claims 5, 6 and 14 state: "wherein the integrated PDK stores local, secured financial information." '188 patent claim 10 states: "wherein the integrated PDK stores local, secured biometric information." '700 patent claim 1 states: "an integrated personal digital key (PDK) for storing local, secured financial information." '700 patent claims 5 and 15 state: "wherein the external PDK stores local, secured financial information." '700 patent claims 6 and 11 state: "wherein the integrated PDK stores local, secured financial information." '700 patent claims 4 and 14 state: "wherein the integrated PDK includes local, secured biometric information for authenticating a user."

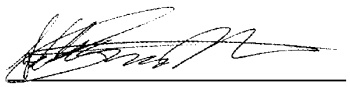
91. Putting together the disclosure of column 14 describing the hybrid device as having a storage area, and that the PDK is described as the part that is used for storing information, this implies a requirement that a hybrid device should have a PDK. This is true for certain embodiments, but not true for the embodiment described in figure 12, which is expressly described as possibly including only a RDC.

92. The claims also fail to clarify the scope of the term "hybrid device." Claim 1 of the '188 patent states: "A hybrid device comprising: an integrated personal digital key (PDK)… and an integrated RDC." Claim 10 of the '188 patent states "the hybrid device including an integrated PDK and the integrated RDC." Identical language is found in '700 patent claims 1 and 11.

93. While the claimed hybrid device is required to have both PDK and RDC, it does not resolve the issue of the scope of the term "hybrid device." In fact, as mentioned above, an unclaimed embodiment has a hybrid device with only a RDC.

94. Because there are problems with any possible interpretation of hybrid device, as described in the paragraphs above, a POSITA would not be able to reasonably conclude what are the boundaries and proper scope of the term "hybrid device." Therefore, it is my opinion that "hybrid device" is indefinite, interpreted in light of the claims, specification and prosecution history, as it fails to inform a POSITA with reasonable certainty about the scope of the invention.

I declare under penalty of perjury that the foregoing is true and correct. Executed in Austin, TX on October 28, 2021.



Dr. Seth James Nielson

Trials@uspto.gov
571-272-7822

Paper 12
Date: February 28, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2021-01447
Patent 9,298,905 B1

Before KEVIN F. TURNER, JUSTIN T. ARBES, and DAVID C. McKONE, *Administrative Patent Judges.*

TURNER, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Petitioner Samsung Electronics America, Inc. filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1–12 of U.S. Patent No. 9,298,905 B1 (Ex. 1001, "the '905 Patent") pursuant to 35 U.S.C. § 311(a). Patent Owner Proxense, LLC filed a Preliminary Response (Paper 10, "Prelim. Resp.") pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." *See* 37 C.F.R. § 42.4(a) ("The Board institutes the trial on behalf of the Director."). For the reasons that follow, we do not institute an *inter partes* review.

B. Related Matters

The parties indicate that the '905 Patent is the subject of *Proxense, LLC v. Samsung Electronics Co., Ltd.*, Case No. 6:21-cv-00210 (W.D. Tex.) ("the district court case"). *See* Pet. 3; Paper 5, 1. Petitioner also filed petitions challenging claims of other patents asserted in the district court case: Cases IPR2021-01438, IPR2021-01439, IPR2021-01444, and IPR2021-01448.

C. The '905 Patent

The '905 Patent discloses systems for "authentication responsive to biometric verification of a user being authenticated," using "a persistent storage to persistently store[] a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format." Ex. 1001, 1:65–67.

The '905 Patent states that "[c]onventional user authentication techniques," such as requiring input of a password, were deficient because they "require[d] the user to memorize or otherwise keep track of the credentials" and "it can be quite difficult to keep track of them all." *Id.* at 1:28–37. Other techniques, such as "provid[ing] the user with an access object . . . that the user can present to obtain access," were inadequate because "authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object." *Id.* at 1:38–46. According to the '905 Patent, there was a need in the art for a system for "verifying a user that is being authenticated that does not suffer from [such] limitations" and "ease[s] authentications by wirelessly providing an identification of the user." *Id.* at 1:55–58.

Figure 2 of the '905 Patent is reproduced below.

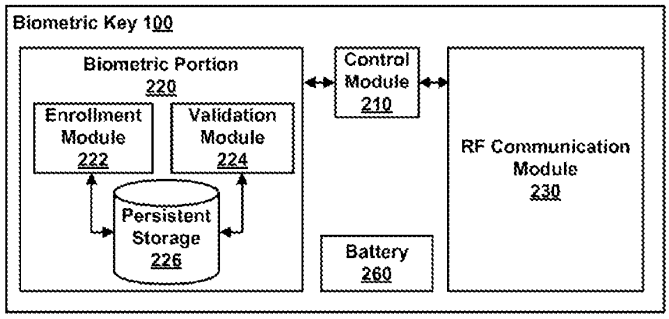


FIG. 2

Figure 2 is a block diagram of the functional modules of a biometric key. Ex. 1001, 3:30–33, 4:42–43. Enrollment module 222 registers a user with biometric key 100 by persistently storing biometric data associated with the user (e.g., a digital image of the retina, fingerprint, or voice sample) in persistent storage 226. *Id.* at 4:67–5:23. Enrollment module 222 registers biometric key 100 with a trusted authority by providing a code, such as a device ID, to the trusted authority or, alternatively, the trusted authority can

provide a code to biometric key 100. *Id.* at 5:3–7. The code is stored in persistent storage 226. *Id.* at 5:24–26. "Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data." *Id.* at 5:31–33. "Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data)." *Id.* at 5:33–36. In a fingerprint embodiment, validation module 224 uses scan pad 120 (shown in Figure 1) to capture scan data from the user's fingerprint and compares the scanned data to the stored fingerprint to determine whether the scanned data matches the stored data. *Id.* at 5:8–12.

The interaction of biometric key 100 with other system components is illustrated in Figure 3, reproduced below.

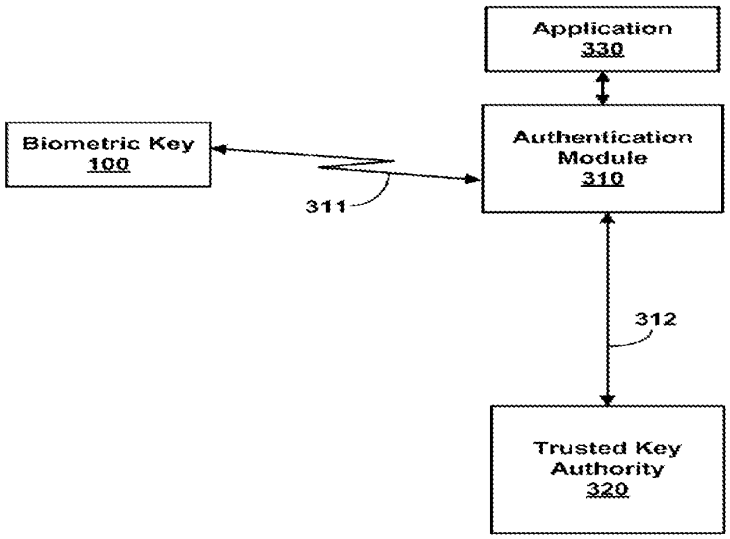


FIG. 3

Figure 3 is "a block diagram illustrating a system for providing authentication information for a biometrically verified user." Ex. 1001,

3:33–35. Authentication module 310 is coupled to biometric key 100 via line 311 (a wireless medium) and with trusted key authority 320 via line 312 (a secure data network such as the Internet). *Id.* at 5:67–6:7. Authentication module 310 requires the device ID code (indicating successful biometric verification) from biometric key 100 before allowing the user to access application 330. *Id.* at 6:10–13. Authentication module 310 provides the device ID code from biometric key 100 to trusted key authority 320 to verify that it belongs to a legitimate key. *Id.* at 6:13–19; *see also id.* 6:39–45 ("In one embodiment, trusted key authority 320 verifies that a code from a biometric key is legitimate. To do so, the trusted key authority 320 stores a list of codes for legitimate biometric keys. . . . In one embodiment, trusted key authority 320 can also store a profile associated with a biometric key."). Authentication module 310 then sends a message to application 330 to allow the user access to the application responsive to a successful authentication by trusted key authority 320. *Id.* at 6:17–19.

"Application 330 can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account . . . and the like." Ex. 1001, 6:21–26. Trusted key authority 320 can be operated by an agent, such as "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at 7:33–36. "The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user." *Id.* at 7:36–39.

D. Illustrative Claim

Challenged claims 1 and 9 of the '905 Patent are independent. Claims 2–8 and 10–12 depend directly or indirectly from claim 1, although the language of certain claims suggests that the Patentee may have intended certain claims to have different dependencies. *See* Pet. 34 (taking no position regarding potential indefiniteness due to the dependencies). Claims 13–18 also issued with the '905 Patent, but are not challenged.

Claim 1 recites (with letter designations used in the Petition (Pet. iv) to refer to the various limitations):

> 1. A method comprising:
>
> [A] persistently storing biometric data of a legitimate user and an ID code on an integrated device;
>
> [B] responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor;
>
> [C] comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
>
> [D] responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and
>
> [E] responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code, allowing the user to complete a financial transaction.

Ex. 1001, 10:11–28.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 5), supported by the declaration of Dr. Andrew Wolfe (Ex. 1003) in support of its contentions:

Claim(s) Challenged	35 U.S.C. §	References/Basis
1, 3–10, 12	103(a)[1]	Scott[2], Lapsley[3]
2, 11	103(a)	Scott, Lapsley, Robinson[4]
1, 3–7, 9, 10, 12	103(a)	Berardi[5], Shreve[6], Kinoshita[7]

[1] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103. Because the challenged claims of the '905 Patent have an effective filing date before the effective date of the applicable AIA amendment, we refer to the pre-AIA version of 35 U.S.C. § 103. *See* Ex. 1001, codes (22), (60).

[2] International Patent Application Publication No. WO 99/56429, published Nov. 4, 1999 (Ex. 1005, "Scott"); when referencing portions of Scott, we refer to the original publication's page numbers in the top-center of each page (not the page numbers added by Petitioner in the lower-right corner of each page), consistent with the parties' usage in their papers.

[3] US Patent Application Publication No. 2001/0000535 A1, published Apr. 26, 2001 (Ex. 1007, "Lapsley").

[4] US Patent Application Publication No. 2003/0177102 A1, published Sept. 18, 2003 (Ex. 1008, "Robinson").

[5] US Patent No. 7,239,226 B2, filed July 9, 2002, issued July 3, 2007 (Ex. 1010, "Berardi").

[6] US Patent Application Publication No. 2002/0109580 A1, published Aug. 15, 2002 (Ex. 1012, "Shreve").

[7] US Patent Application Publication No. 2003/0055792 A1, published Mar. 20, 2003 (Ex. 1013, "Kinoshita").

II. ANALYSIS

A. Discretionary Denial Under 35 U.S.C. § 314(a)

Institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) ("[T]he PTO is permitted, but never compelled, to institute an [*inter partes* review (IPR)] proceeding."); 35 U.S.C. § 314(a) ("The Director *may not* authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." (emphasis added)). In the Preliminary Response, Patent Owner argues that we should exercise our discretion to deny the Petition in view of the district court case, where Petitioner previously asserted that we should not exercise our discretion to deny institution. Prelim. Resp. 4–6; Pet. 13–19. We need not decide this issue, however, as we determine that Petitioner has not shown a reasonable likelihood that it would prevail with respect to at least one of the challenged claims.

B. Legal Standards

A claim is unpatentable for obviousness if, to one of ordinary skill in the pertinent art, "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a) (2006)). The question of obviousness is resolved on the basis of underlying factual determinations, including "the scope and content of the prior art"; "differences between the prior art and the claims at issue"; and "the level of

ordinary skill in the pertinent art." *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Additionally, secondary considerations, such as "commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy." *Id.* When conducting an obviousness analysis, we consider a prior art reference "not only for what it expressly teaches, but also for what it fairly suggests." *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1049 (Fed. Cir. 2019) (citation omitted).

A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. An obviousness determination requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citation omitted); *see KSR*, 550 U.S. at 418 (for an obviousness analysis, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does").

"Although the *KSR* test is flexible, the Board 'must still be careful not to allow hindsight reconstruction of references . . . without any explanation as to *how* or *why* the references would be combined to produce the claimed invention.'" *TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1066 (Fed. Cir. 2016) (citation omitted). Further, an assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *accord In re NuVasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (stating that "conclusory statements" amount to an "insufficient articulation[] of motivation to combine"; "instead, the finding must be supported by a 'reasoned explanation'" (citation omitted)); *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) ("To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.").

C. Level of Ordinary Skill in the Art

Petitioner argues that at the time of the '905 Patent, a person of ordinary skill in the art would have had "a bachelor's degree in computer or electrical engineering (or an equivalent degree) with at least three years of experience in the field of encryption and security (or an equivalent)." Pet. 4. Patent Owner does not address the level of ordinary skill in the art in its Preliminary Response. Based on the record presented, including our review of the '905 Patent and the types of problems and solutions described in the '905 Patent and cited prior art, we adopt Petitioner's definition of the level of ordinary skill in the art and apply it for purposes of this Decision.

D. Claim Interpretation

We interpret the challenged claims

> using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b) (2021). "In determining the meaning of [a] disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006). Claim terms are generally given their ordinary and customary meaning as would be understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Petitioner submits that no express interpretations of any claim terms are necessary to resolve the parties' dispute and "the claim terms should be given their plain and ordinary meaning." Pet. 7. Patent Owner identifies two claim terms, "third-party trusted authority" and "access message," both recited in independent claims 1 and 9, that it presents as being edifying, based on Petitioner's Opening Claim Construction Brief in the district court case (Ex. 2001), and its own Responsive Claim Construction Brief (Ex. 2002). Prelim. Resp. 2–4.

Patent Owner points out that Petitioner argued in the district court case that a "third-party" is "an entity with a responsibility separate from executing the transaction itself." Prelim. Resp. 2 (quoting Ex. 2001, 7). In the district court case, Petitioner argued that no construction of "third-party trusted authority" was needed and "[t]he intrinsic evidence does not suggest

a party or component numbered after a second party." Ex. 2001, 6–7. This was in response to its articulation of Patent Owner's position, namely, that a "third-party trusted authority" is "[a] third component that provides a second level of authentication." *Id.* at 6.[8]

Petitioner further argued that "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation," and "[t]he applicant emphasized the prior art 'disclose[d] two parties: the user and the institution.'" Ex. 2001, 7 (quoting remarks made by the applicant for a related patent accompanying an amendment and addressing the same claim term) (alterations by Petitioner). Petitioner argued that "the intrinsic evidence suggests 'third party' relates to a specific class of entity occupying the aforementioned particular relationship." *Id.* Petitioner then pointed out that "the [S]pecification [of the related patent] explains the agent for the trusted authority 'can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness.'" *Id.* According to Petitioner, "[t]his 'witness' role further aligns with prosecution history where the applicant explained 'sending a code to a receiver of a *door that the user is trying to access*' does not satisfy the 'third party' limitation." *Id.* (quoting an amendment in the related patent file history).

[8] In its responsive brief, Patent Owner changed its position with respect to the terms "third-party trusted authority" and "agent" to "[n]o construction needed" and stated that it "no longer seeks to submit th[e] term[s] for construction." Ex. 2002, 12. The district court did not construe the terms. Ex. 3001.

Petitioner further offered expert testimony in the district court case to support an argument that "[c]ommon industry use of 'trusted third party' identifies 'third party' as an entity with a responsibility separate from executing the transaction itself." *Id.* at 7–8 (citing a declaration of Seth James Nielson, Ph.D. (Ex. 2003 ¶¶ 70–74) and a book, CRYPTOGRAPHIC LIBRARIES FOR DEVELOPERS). Dr. Nielson appears to best articulate the distinction Petitioner was drawing between a third component and a third entity: "the [S]pecification, the prosecution history, and common industry usage all suggest a 'third party' refers to an entity outside of the transaction or a witness thereto rather than a 'third component.'" Ex. 2003 ¶ 74.

In light of Petitioner's arguments in the district court case, Patent Owner contends that the parties "agree that a 'third-party trusted authority' is an institution or entity that is outside of the multi-party system (user and application or vendor) that is being authenticated." Prelim. Resp. 3.

We agree with Patent Owner. The plain meaning of "third-party trusted authority" suggests an entity or party separate from the principal parties to a transaction. *See, e.g.*, THE AMERICAN HERITAGE COLLEGE DICTIONARY 1433 (4th ed. 2004) ("third party n. . . . 2. One other than the principals involved in a transaction.") (Ex. 3002).

This is consistent with the description in the Specification. For example, Figure 3, reproduced above, depicts trusted key authority 320 as an entity separate from biometric key 100, authentication module 310, and application 330. As the Specification states, "[t]rusted key authority 320 is a third-party authority that is present in some embodiments in order to provide enhanced security." Ex. 1001, 6:37–39. Examples of trusted key authorities include "a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness." *Id.* at

7:33–36. Petitioner's citations to the applicant's statement during prosecution of the related patent also are consistent with a third-party trusted authority being an entity separate from the principal parties to a transaction, as is the declaration of Dr. Nielson. *See* Ex. 2001, 6–8; Ex. 2003 ¶¶ 70–74. Thus, we interpret "third-party trusted authority" to mean a trusted authority that is an entity separate from the parties to a transaction.

Claim 1 also recites "responsive to receiving an access message from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," with claim 9 providing a similar recitation. Patent Owner argues that "[a]n 'access message' must be sent by the 'third party trusted authority'" and the parties "agree that the 'access message' originates from the 'third-party trusted authority' and communicates information regarding authentication." Prelim. Resp. 3–4 (citing Ex. 2001, 9). Given the express requirement in claims 1 and 9 that the access message be received "from" the third-party trusted authority, we conclude that no further interpretation of the "access message" limitations is necessary.[9]

E. Obviousness Ground Based on Scott and Lapsley

Petitioner contends that claims 1, 3–10, and 12 are unpatentable over Scott and Lapsley under 35 U.S.C. § 103(a). Pet. 19–34. Patent Owner argues that the Petition fails to demonstrate that the combination of references teaches or suggests all elements of the challenged claims. Prelim.

[9] Petitioner argued in the district court case that the limitations mean "[r]eceiving a signal from the agent permitting a user to access an application," Patent Owner argued that no construction was necessary and the phrases should be given their plain and ordinary meaning, and the district court determined that no construction was necessary. Ex. 3001, 3.

Resp. 6–9. We are not persuaded that Petitioner has established a reasonable likelihood of prevailing on this asserted ground as to any of the challenged claims. We begin with short discussions of Scott and Lapsley, and discuss Petitioner's contentions and Patent Owner's arguments thereafter.

1. Scott

Scott describes "a portable personal identification device for providing secure access to a host facility" in which the device "includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and provid[es] a biometric signal indicative thereof." Ex. 1005, 2:5–8. Figure 1 of Scott, reproduced below, illustrates an example.

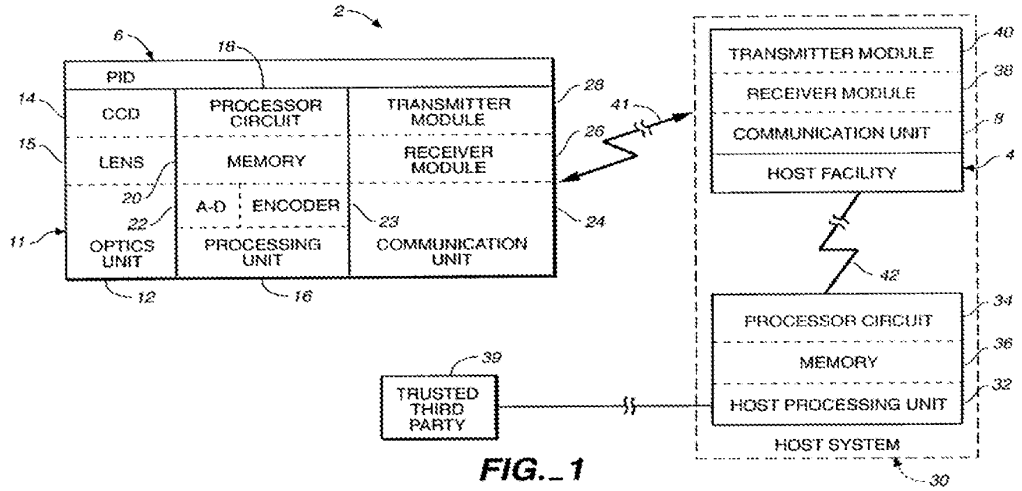


FIG._1

Figure 1 is a block diagram of security system 2 that provides access to host facility 4 (e.g., a bank, store, military base, computer system, automobile, home security system, or gate). *Id.* at 10:1, 24–28.

A registered person carries battery powered personal identification device (PID) 6 (e.g., similar in size to a hand-held pager), which includes biometric sensor 11. *Id.* at 10:28–11:5. Memory 20 stores an ID code that is set in PID 6 by the manufacturer. *Id.* at 11:11–13. The owner of PID 6

enrolls into the unit by scanning a finger using biometric sensor 11 to create an image that is stored as the fingerprint template in memory 20. *Id.* at 11:14–20, 15:30–16:6. PID 6 communicates wirelessly via transmission signal 41 with host facility 4. *Id.* at 12:14–16.

Host facility 4 is part of host system 30 (e.g., a bank ATM system or point of sale system), which also includes host processing unit 32. *Id.* at 11:31–12:2. "Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42." *Id.* at 12:3–5. "Memory 36 stores ID codes of enrolled individuals who have registered with host system 30." *Id.* at 12:6–7.

Figure 7 of Scott is reproduced below.

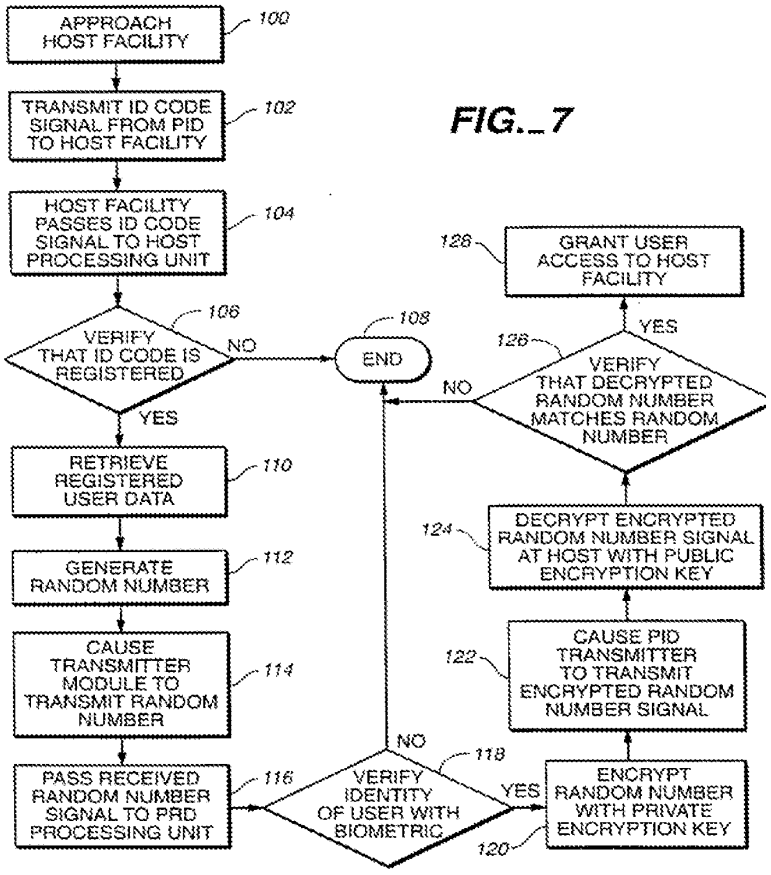


FIG._7

Figure 7 is a flow diagram of a method of accessing a host facility with a personal identification device. *Id.* at 10:13–14.

A user with PID 6 approaches host facility 4 (e.g., an ATM) and transmits the ID code to host receiver module 38, which passes it to host processing unit 32. *Id.* at 17:20–27 (steps 100–104). Host processing unit 32 verifies that the received ID code represents a registered ID code and, if so, the account or user information is located. *Id.* at 17:27–30 (steps 106, 110). Host processing unit 32, via transmitter module 40, sends a random number to PID 6, in response to which PID 6 performs a user verification. *Id.* at 18:1–4 (steps 112–118). PID 6 verifies the user's fingerprint when the user places their finger on platen 15 of biometric sensor 11 by comparing the

fingerprint signal to the stored fingerprint template. *Id.* at 16:19–29. If PID 6 successfully verifies the user's fingerprint, PID 6 encrypts the random number and sends it back to host processing unit 32, which decrypts the random number and verifies that it matches the random number it sent to PID 6. *Id.* at 18:5–14 (steps 120–126). If the random number is a match, host processing unit 32 grants the user access to host facility 4. *Id.* at 18:14–15 (step 128).

2. Lapsley

Lapsley describes "a system and method of using biometrics for processing electronic financial transactions such as on-line debit, off-line debit and credit transactions without requiring the user to directly use or possess any man-made tokens such as debit or credit cards or checks." Ex. 1007 ¶ 2.

Figure 2 of Lapsley, reproduced below, illustrates an example.

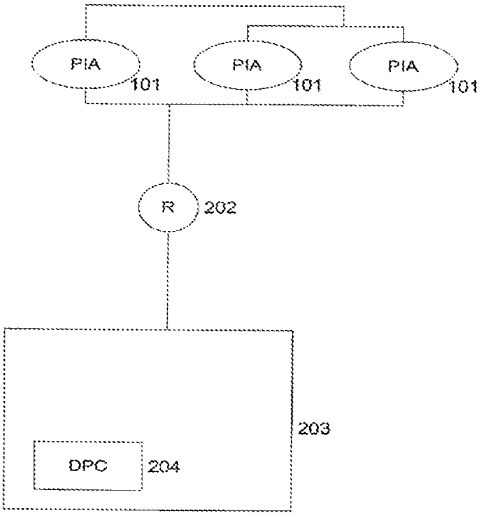


Figure 2 is a block diagram showing the connections among Party Identification Devices (PIAs) 101, router 202, and Network Operations Center (NOC) 203. *Id.* ¶ 47. Figure 2 is in the context of a supermarket

chain or other multi-lane retail chain with multiple PIAs 101 connected via an in-store local area network to local router 202, which is connected to NOC 203 via frame relay lines. *Id.* ¶ 98. NOC 203 includes Data Processing Center (DPC) 204. *Id.*

Each PIA 101 has a hardware identification code that is assigned to it and registered with DPC 204 at the time of manufacture, making the PIA uniquely identifiable to DPC 204 in transmissions from the PIA. *Id.* ¶¶ 85, 161. An entity uses the PIA hardware identification code to identify itself to the DPC. *Id.* ¶ 158.

Figure 7 of Lapsley is reproduced below.

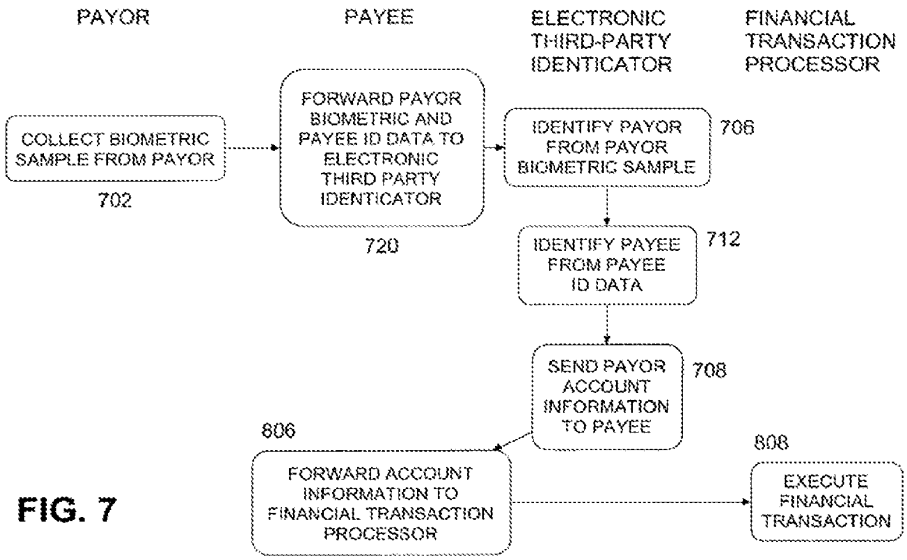


FIG. 7

Figure 7 is a flow diagram showing a transaction flow among the participants in a retail point-of-sale transaction. *Id.* ¶¶ 52, 166.

The customer/payor originates an electronic payment at a point-of-sale by submitting a bid biometric sample obtained by a biometric sensor of the PIA controlled by a payee/seller. *Id.* ¶¶ 166–167 (step 702). The PIA determines that the sample is not fraudulent and sends the sample to the DPC. *Id.* ¶ 167. The payor enters a PIN code into the PIA, and the

PIA transmits the biometric data, PIN, and hardware identification code of the PIA to the DPC. *Id.* ¶ 168 (step 720). The DPC identifies the payor using the biometric sample, retrieves a list of financial accounts that the payor has registered with the system, and transmits the list to the PIA. *Id.* (steps 706, 708). The DPC identifies the payee using the PIA hardware identification code. *Id.* ¶¶ 166, 168. The payor selects a financial account at the PIA, and the PIA transmits the financial information to the payee's in-store payment system (e.g., point-of-sale terminal or electronic cash register). *Id.* ¶¶ 169–170. The in-store payment system authorizes the transaction. *Id.* ¶ 170.

3. Claim 1

Petitioner argues that Scott and Lapsley collectively teach all of the limitations of claim 1. Pet. 19–26. With respect to the preamble of claim 1, Petitioner contends that Scott teaches a method of verifying a user during authentication of an integrated device (i.e., PID 6). *Id.* at 19.

With respect to limitation A, Petitioner argues that Scott teaches persistently storing "biometric data of a user" in memory 20 of PID 6 and persistently storing a plurality of codes and other data values including an ID code that uniquely identifies PID 6, where the ID code may be set by the device manufacturer and can be the device serial number. Pet. 20–21 (citing Ex. 1005 4:1–18, 6:28–7:23, 8:13–22, 11:11–20, 13:10–15, 15:30–16:6, 19:30–32).

With respect to limitation B, Petitioner argues that Scott discloses receiving a request for a biometric verification of the user by pressing a "verify" button on PID 6, and in response to this request, PID 6 can receive scan data from a biometric scan, such as a fingerprint scan from the user

placing a finger on platen 15, a voice biometric scan, "or any other type of biometric scan." Pet. 21–22 (citing Ex. 1005, 3:21–32, 16:19–29, Fig. 4A).

With respect to limitation C, Petitioner argues that Scott discloses that after receiving the biometric scan data, PID 6 compares the received biometric scan data (e.g., voice, iris, or fingerprint biometric) to a stored biometric template in order to verify the user's identity. Pet. 22 (citing Ex. 1005, 15:30–16:29).

With respect to the first portion of limitation D, Petitioner relies on the teachings of Scott. Pet. 22–23. As to the limitation of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code," Petitioner contends that, in response to the comparison discussed in connection with limitations B and C above, Scott's PID 6 wirelessly transmits to host facility 4 "an encrypted message with [the] ID code and other data such as a synchronization counter." *Id.* (citing Ex. 1005, 4:6–18, 5:22–6:24, 6:28–7:23).

With respect to the second portion of limitation D, namely "for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," Petitioner contends that "Scott discloses that the third-party trusted authority host processing unit 32 stores a list that includes an ID code and a public key for each registered PID 6," and host processing unit 32 compares the device ID code received from PID 6 to this list to authenticate PID 6 as a legitimately registered device. *Id.* at 23–24 (citing 5:10–21, 6:11–21, 7:24–8:4, 8:18–22; 9:23–25, 11:12–13, 12:6–13, 13:10–15, 19:18–20, 30–32, Fig. 1). Although not cited in the Petition, Dr. Wolfe repeats these arguments in his testimony. *See* Ex. 1003 ¶ 45. Petitioner and Dr. Wolfe thus identify Scott's host processing unit 32 as corresponding to the claimed

"third-party trusted authority." Also, in its analysis of limitation E of claim 1, Petitioner makes clear that host facility 4 is the application (e.g., key card entry, ATM machine, garage door opener) that is accessed when the transaction is completed. Pet. 26 (citing Ex. 1005, 17:20–18:19, 5:10–21, 8:5–12).

Patent Owner argues that "host processing unit 32 is *part of* the system being accessed—it is not a third party." Prelim. Resp. 7 (citing Ex. 1005, 11:24–25, 11:30–12:1). As explained above, a "third-party trusted authority" is a trusted authority that is an entity separate from the parties to a transaction. *See supra* Section II.D. Scott describes both host processing unit 32 (the alleged "third-party trusted authority") and host facility 4 (the alleged application to be accessed by the user, "selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file") as part of a single entity, host system 30. Ex. 1005, 11:31–12:5 ("Host facility 4 is part of a host system 30. Host system 30 will typically be bank ATM systems, point of sale systems, and the like. Host system 30 also includes a host processing unit 32, which has a processor circuit 34 and memory 36 . . . . Host processing unit 32 may be located with host facility 4, or may be located at a remote location, where it may also serve other host facilities 4 in a distributed network 42."). As such, host processing unit 32, because it is not an entity separate from host facility 4, is not a third-party trusted authority.

Petitioner further argues that, "[t]o the extent [that Patent Owner] argues that Scott's host processing unit 32 is not a third-party trusted authority, Lapsley . . . provides additional disclosure rendering this feature of the limitation obvious to a [person of ordinary skill in the art]." Pet. 24.

Petitioner contends that Lapsley's DPC is a trusted third-party authority that receives biometric data and a hardware identification code from a PIA and uniquely identifies the PIA by finding the identification code on a list the DPC maintains. *Id.* at 24–25 (citing Ex. 1007 ¶¶ 54, 82, 85, 103, 104, 158, 161, 166–168).

Relying on Dr. Wolfe's testimony, Petitioner argues that a person of ordinary skill in the art

> would have been motivated to modify Scott's system such that authentication is performed by an external third-party trusted authority possessing a list of device ID codes that unique[ly] identify legitimate PIDs, as taught in Lapsley, to improve efficiency and flexibility of the system by consolidating ID codes to a central location at a secure third-party agent.

Pet. 25 (citing Ex. 1003 ¶ 47). Dr. Wolfe repeats this argument in his testimony, but does not state the basis for his opinion, rendering it of little value. *See* 37 C.F.R. § 42.65(a). Citing to Lapsley, Petitioner argues that an ordinarily skilled artisan "would have recognized the benefit in reducing the risk of fraud by improving security and authentication by using a trusted third-party agent to verify devices involved in a transaction." *Id.* (citing Ex. 1007 ¶¶ 8, 9, 27, 29). Petitioner argues that an ordinarily skilled artisan "would have further understood that it was common to have an ATM that is not owned by a bank use the bank as a third party for authorization and it was common for a store to use a bank or credit card exchange as a third party for authorization." *Id.* at 26. Petitioner does not cite any evidence for this argument.

Patent Owner responds that "Lapsley's DPC is part of the system providing access to a user's registered financial accounts, *i.e.*, a cloud based digital wallet—not a *third party* trusted authority." Prelim. Resp. 8 (citing

Ex. 1007 ¶¶ 102, 138, 139). Patent Owner contends that, "[i]n Lapsley, instead of using a personal fob or phone to access the DPC digital wallet, the user utilizes a Party Identification Apparatus located at a store." *Id.* at 8–9 (citing Ex. 1007 ¶¶ 167–169). According to Patent Owner, "[a]s the DPC is accessed with the PIA to retrieve a list of user financial accounts stored in the DPC, the DPC must be the system being accessed/authenticated. Consequently, Lapsley's DPC is not what the Petitioner and Patent Owner agree constitutes a 'third-party trusted authority.'" *Id.* at 9.

We agree with Patent Owner. Petitioner has not explained sufficiently why Lapsley's DPC is a third-party trusted authority, what entities the DPC is a third-party relative to, or what application the user is being permitted to access in the asserted combination. As Patent Owner points out, the DPC appears to be what is being accessed, as the payee and payor, with the PIA, access a list of financial accounts from the DPC. *See id.* at 8–9; Ex. 1007 ¶¶ 167–170. Here, the DPC is the resource to be accessed, but it is a party to the transaction, rather than a third party. This is similar to the situation Petitioner argues that the applicant distinguished during prosecution: "[d]uring prosecution, the applicant explained a 'user []prov[ing] to the same institution that authenticates the fingerprint information that the user is who he purports to be' does not satisfy the 'third party' limitation." *See* Ex. 2001, 7 (quoting remarks made by the applicant during prosecution of the related patent (alterations by Petitioner)).

Petitioner's reasons to combine also are conclusory and unsupported by persuasive evidence. In particular, Dr. Wolfe merely repeats Petitioner's arguments in his testimony, without further explaining them or identifying

the basis for his opinions.[10] *See* Ex. 1003 ¶ 48. We agree with Patent Owner that Petitioner has not shown that Lapsley teaches a "third-party trusted authority" or that a skilled artisan would have had reasons, with rational underpinning, to combine the teachings of Scott and Lapsley.

Because Petitioner does not show persuasively that either Scott or Lapsley teaches a "third-party trusted authority," as recited in claim 1, or that an ordinarily skilled artisan would have combined the teachings of those references, Petitioner has not shown sufficiently that Scott and Lapsley teach limitation D:

> responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority.

Petitioner's ground fails for an additional reason as well. The claim plainly requires that the access message be received "from the third-party trusted authority," per limitation E.

Petitioner argues that "in response to authentication of the received ID code by comparing it to a stored ID code, the receiver module 26 of PID 6 receives a random number signal from [host processing unit 32] that enables access to a secure resource." Pet. 26 (citing Ex. 1005, 5:10–21, 8:5–12, 17:20–18:19). Petitioner does not provide any further explanation as to why Scott's host processing unit 32 allegedly constitutes a "third-party trusted authority." *See id.* Nor does Petitioner mention Lapsley, or the combined teachings of Scott and Lapsley, in addressing limitation E of claim 1. *See id.* Because Petitioner has not shown sufficiently that host processing unit 32 is

[10] Moreover, as explained below, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight. *See infra* Section II.G.

a "third-party trusted authority," Petitioner likewise has not established that Scott's random number signal is an "access message [sent] from the third-party trusted authority-indicating that the third-party trusted authority successfully authenticated the ID code," as recited in limitation E of claim 1. *See* Prelim. Resp. 9.

Therefore, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claim 1 is unpatentable over Scott and Lapsley.

4. Claims 3–10 and 12

Independent claim 9 recites the same elements of independent claim 1, discussed above, that we determine that Petitioner's Petition has not shown according to this ground of unpatentability. *See* Ex. 1001, 10:54–11:3. Claims 3–8 and 10–12 ultimately depend from claim 1. For the reasons explained above regarding claim 1, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 3–10 and 12 are unpatentable over Scott and Lapsley.

F. Obviousness Ground Based on Scott, Lapsley, and Robinson

Petitioner contends that claims 2 and 11 are unpatentable over Scott, Lapsley, and Robinson under 35 U.S.C. § 103(a). Pet. 34–36. Claims 2 and 11 ultimately depend from claim 1. Petitioner does not argue that the additional reference (Robinson) teaches the missing limitations of parent claim 1, as discussed above. *See id.* Accordingly, for the reasons explained above, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 2 and 11 are unpatentable.

G. Obviousness Ground Based on Berardi, Shreve, and Kinoshita

Petitioner contends that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita under 35 U.S.C. § 103(a), citing the testimony of Dr. Wolfe as support. Pet. 36–46 (citing Ex. 1003).

Petitioner's allegations and citations to Berardi do not correspond to the disclosure of that reference. *See* Prelim. Resp. 10 ("With regard to Berardi, Petitioner references elements and paragraphs not contained within Berardi at all, *i.e.*, in error.").[11]

For example, in alleging that Berardi teaches "responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority," as recited in limitation D of claim 1, Petitioner argues that "issuer system 1010 [that] includes an issuer account server (IAS) 1014 that processes fob identifying information," of Berardi, corresponds to the claimed "third-party trusted authority." Pet. 38–39 (citing Ex. 1010, 10:56–11:12, 22:1–41, 28:50–67). Berardi does not describe an "issuer system 1010" or "issuer account server (IAS) 1014." The cited material in columns 10 and 11 is inapposite (and does not discuss issuer system 1010 or IAS 1014), Berardi ends its disclosure at line 30 (not line 41) of column 22, and column 28 does not exist in Berardi. Additionally, following the normal

[11] Patent Owner notes that Petitioner's errors "make[] it difficult to ascertain Petitioner's argument[s]," but argues that "a full reading of Berardi makes clear that it fails to disclose a 'third-party trusted authority.'" Prelim. Resp. 10. Patent Owner then presents substantive arguments as to Berardi, Shreve, and Kinoshita. *Id.* at 10–15. We deny the Petition as to this ground based on Petitioner's failure to present an understandable case as to Berardi and do not reach Patent Owner's additional arguments.

numbering of elements in patent drawings, the highest number referenced in Berardi is "906," short of the elements "1010" and "1014," discussed by Petitioner.

Also in its analysis of limitation E of claim 1, Petitioner states that Berardi discloses that "in response to authentication of the received identifying information of the fob 102, the POS device 110 may send 'an optical and/or audible transaction status message' to the RFID reader 104 for communication directly with the customer." Pet. 40–41 (citing Ex. 1010, 20:51-62, Fig. 8). Column 20, lines 51–62 of Berardi encompass a portion of claim 1 of Berardi, and the cited section does not discuss POS Device 110. Figure 8 of Berardi provides a flow diagram of an exemplary payment/transaction process, but does not detail sending an optical and/or audible message, as Petitioner alleges. We conclude that Petitioner did not simply misidentify or mislabel the components of Berardi it sought to reference.

There are numerous similar errors. For example, Petitioner relies on column 28, lines 50–67, which does not exist in Berardi, for limitations A, B and D of claim 1. *See* Pet. 37–39. Petitioner's citation to column 12, lines 36–41 in its analysis of limitation B of claim 1 does not correspond to biometric information, or anything else we can discern to be relevant to these limitations. *See id.* at 38. Instead, it discusses RFID reader 104 authenticating fob 102. Ex. 1010, 12:36–41. We do not intend to list all such errors here. We decline to speculate as to what Petitioner might have intended to cite. The result of the errors in the Petition is that we are unable to understand Petitioner's allegations and Patent Owner cannot fairly be said to be on notice of Petitioner's challenge based on Berardi.

Petitioner contends that (1) to the extent Berardi fails to teach limitation D of claim 1, Shreve provides additional disclosure; and (2) to the extent Berardi fails to teach limitation E of claim 1, Kinoshita provides additional disclosure. Pet. 39–41. However, because Petitioner has not sufficiently explained its allegations as to Berardi, it is impossible to understand Petitioner's proposed combination with Shreve and Kinoshita. Moreover, as explained above, Petitioner's arguments regarding limitations A, B, D, and E of claim 1 are based largely on material that does not exist in Berardi. Thus, even if we were able to discern Petitioner's arguments for limitations A, B, D, and E of claim 1, Petitioner's cited evidence does not support its allegations for other elements of claim 1.

Petitioner's allegations for independent claim 9 largely track or refer back to its analysis of claim 1 and, thus, suffer from the same defects. *See* Pet. 44–46. Petitioner's allegations for dependent claims 3–7, 10, and 12 do not shed any additional light on what Petitioner might have intended for claim 1, and instead largely cite irrelevant or non-existent material in Berardi. *Id.* at 42–44, 46.[12]

[12] We also express concern with Dr. Wolfe's testimony. Paragraphs 71–97 of his declaration (Exhibit 1003) appear to be a near carbon copy of pages 36–46 of the Petition, and include the Petition's citations to obviously incorrect or non-existent material in Berardi. These circumstances suggest a lack of attention, as even a cursory review would have shown that his testimony regarding Berardi includes numerous references to irrelevant or non-existent material, rendering that testimony not useful. This is not an instance of one or even a few inadvertent errors that might go missed upon a diligent review. The entirety of Dr. Wolfe's testimony regarding Berardi is defective on its face. For these reasons, the entirety of Dr. Wolfe's testimony lacks credibility and is entitled to little or no weight.

In sum, we cannot discern Petitioner's allegations of obviousness based on Berardi, Shreve, and Kinoshita, nor can we say Patent Owner is on notice of those allegations. Accordingly, Petitioner has not shown a reasonable likelihood of prevailing on its assertion that claims 1, 3–7, 9, 10, 12 are unpatentable over Berardi, Shreve, and Kinoshita.

III. CONCLUSION

Based on the arguments presented in the Petition, we conclude that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to at least one claim of the '905 Patent challenged in the Petition. Therefore, we do not institute an *inter partes* review.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied and no *inter partes* review is instituted.

FOR PETITIONER:

James M. Glass
Marissa Ducca
Richard Lowry
Sean Gloth
QUINN EMANUEL URQUHART & SULLIVAN, LLP
jimglass@quinnemanuel.com
marissaducca@quinnemanuel.com
richardlowry@quinnemanuel.com
seangloth@quinnemanuel.com

FOR PATENT OWNER:

David L. Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/015,053	06/08/2022	9298905	2090-0002-REX	7424

142179 7590 08/02/2022

Hard IP LLC (General)
10 Notch Hill Drive
Livingston, NJ 07039

EXAMINER	
RIMELL, SAMUEL G	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
08/02/2022	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

Marissa Ducca
Quinn Emanuel Urquhart & Sullivan
1300 I Street, Suite 900
Washington, DC 20005

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/015,053* .

PATENT UNDER REEXAMINATION *9298905* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Order Granting Request For Ex Parte Reexamination	Control No. 90/015,053	Patent Under Reexamination 9298905	
	Examiner SAM RIMELL	Art Unit 3992	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed 06/08/2022 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☑ PTO/SB/08, c)☐ Other: ____

1. ☑ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

cc:Requester (if third party requester)

DECISION GRANTING EX PARTE REEXAMINATION

The Request filed June 8, 2022 alleges that substantial questions of patentability (SNQ) affecting claims 1-18 of the U.S. Patent Number 9,298,905 are raised by the following prior art references:

Prior Art

Ex. 1005	U.S. Patent No. 7,188,110 ("Ludtke")
Ex. 1006	U.S. Patent Publication No. 2003/0196084 ("Okereke")
Ex. 1007	U.S. Patent Publication No. 2003/0177102 ("Robinson")
Ex. 1008	International Publication Number WO 99/56429 ("Scott")

Brief Overview of US Patent 9,298,905

The invention pertains to systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

Prosecution History of US Patent 9,298,905

US Patent 9,298,905 resulted from the filing of US application 14/521,982 filed October 23, 2014, with a priority claim extending to provisional application 60/637,538 filed December 20, 2004.

The USPTO mailed a non-final office action on June 12, 2015. Claims 11 and 15 were rejected under the provisions of non-statutory double patenting. Claims 2-10 were rejected under 35 USC §101. Claims 2-10 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126). Claims 3 and 13 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126) and Schlotterbeck (US Pre-Grant Publication 2004/0128162). Claims 11-12 and 14-18 were rejected under 35 USC §103 in view of Hsu et al (US Patent 6,041,410) and Stanko (US provisional application 2005/0074126) and Lake (US Pre-Grant publication 2002/0091646).

On September 14, 2015, applicant submitted aa reply with amendments and remarks.

On December 16, 2015, the USPTO issued a Notice of Allowance with claims 2-7 and 9-20 allowed and claims 1 and 8 cancelled. These were subsequently re-numbered as claims 1-18.

The reasons for patentability read as follows:

"The closest prior arts cited are generally directed to various aspects of authenticating users using biometric information. However, none of the cited arts found alone or in combination suggests or teaches all the elements of the independent claims. For instance, no parts of the cited arts teach or suggest limitations such as persistently storing biometric data of a legitimate user and an ID code on an integrated device; responsive to receiving a request for a biometric verification of a user, receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor; comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; responsive to a determination that the scan data matches the biometric data, wirelessly sending the ID code for comparison by a third- party

trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority; and responsive to receiving an access message from the third-party trusted authority indicating that the third-party trusted authority successfully authenticated the user as the legitimate user based on the comparison of the ID code, allowing the user to complete a financial transaction. Therefore, the claims are allowable for the above reason."

Inter Partes Review before Patent Trial and Appeal Board

The records of the Patent Trial and Appeal Board contain the following *Inter Partes* Review Proceedings involving claims of US Patent 9,298,905:

AIA Review #	Filing Date	Institution Decision Date	Petitioner App #	Petitioner Patent #	Petitioner Tech Center	Petitioner	PO/Respondent App #	PO/Respondent Patent #	PO/Respondent Tech Center	PO/Respondent	Status
IPR2021-01447	08/26/2021	02/28/2022				SAMSUNG ELECTRONICS AMERICA, INC	14521982	9298905	2400	Proxense, LLC	Institution Denied

Final Decisions in the Federal Circuit

There are no known final decisions in the Federal Circuit involving US Patent 9,298,905.

Applicability of "Old Art" in Reexamination Proceedings

In the examining stage of a reexamination proceeding, the examiner will consider whether the claims are subject to rejection based on art. Before making such a rejection, the examiner should check the patent's file history to ascertain whether the art that will provide the basis for the rejection was previously cited/considered in an earlier concluded Office examination of the patent (e.g., in the examination of the application for the patent). For the sake of expediency, such art is referred to as "old art" throughout, since the term "old art" was coined by the Federal Circuit in its decision of *In re Hiniker*, 150 F.3d 1362, 1365-66, 47 USPQ2d 1523, 1526 (Fed. Cir. 1998).

If the rejection to be made by the examiner will be based on a combination of "old art" and art newly cited during the reexamination proceeding, the rejection is proper, and should be made.

See *In re Hiniker*, 150 F.3d at 1367, 47 USPQ2d at 1527. (Court held the reexamination proceeding was supported by a substantial new question of patentability where the rejection before the court was based on a combination of art that had been before the examiner during the original prosecution, and art newly cited during the reexamination proceeding.)

For a reexamination that was ordered on or after November 2, 2002 (the date of enactment of Public Law 107-273; see Section 13105, of the Patent and Trademark Office Authorization Act of 2002), reliance solely on old art (as the basis for a rejection) does not necessarily preclude the existence of a substantial new question of patentability (SNQ) that is based exclusively on that old art. Determinations on whether a SNQ exists in such an instance shall be based upon a fact-specific inquiry done on a case-by-case basis. For example, a SNQ may be based solely on old art where the old art is being presented/viewed in a new light, or in a different way, as compared with its use in the earlier concluded examination(s), in view of a material new argument or interpretation presented in the request.

Discussion of SNQs

Issue #1

Requester proposes that Ludtke in view of Okereke raise a substantial new question of patentability (SNQ) with respect to claims 1, 3-10 and 12-18. From this claim set, claims 1, 9, and 13 are the independent claims.

Independent claim 1 recites:

"*receiving, from a biometric sensor, scan data from a biometric scan performed by the biometric sensor; comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; responsive to a determination that the scan data matches the*