

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: David Wyatt
U.S. Patent No.: 11,328,286 Attorney Docket No.: 39843-0147PS1
Issue Date: May 10, 2022
Appl. Serial No.: 16/854,829
Filing Date: April 21, 2020
Title: MULTI-FUNCTION ELECTRONIC PAYMENT CARD AND
DEVICE SYSTEM

Mail Stop Patent Board

Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR POST GRANT REVIEW OF U.S. PATENT NO. 11,328,286
PURSUANT TO 35 U.S.C. §§ 321–329

TABLE OF CONTENTS

I.	REQUIREMENTS FOR PGR.....	1
A.	Grounds for Standing.....	1
B.	The '286 patent is an AIA patent and therefore eligible for PGR.....	1
C.	Challenge and Relief Requested.....	6
D.	Claim Construction.....	8
1.	Claim limitations directed to printed matter are not entitled to patentable weight (claims 1, 5, 15, 19, 20)	8
2.	Additional non-limiting claim features	9
E.	Level of Ordinary Skill in the Art.....	10
II.	THE '286 PATENT.....	10
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	11
A.	GROUND 1A – Claims 1, 2, 7-10, 12-16, and 18 are obvious over Smith in view of Kobylkin, and Gomez	11
1.	Overview of Smith	11
2.	Overview of Kobylkin.....	12
3.	Overview of Gomez	13
4.	The combination of Smith, Kobylkin, and Gomez	13
5.	Reasons to combine Smith, Kobylkin, and Gomez	15
6.	Analysis	21
B.	GROUND 1B – Claims 3 is obvious over Smith in view of Kobylkin, Gomez, and Saarisalo	51
1.	Overview of Saarisalo	51
2.	The combination of Smith, Kobylkin, Gomez, and Saarisalo	52
3.	Reasons to combine Smith, Kobylkin, Gomez, and Saarisalo.....	52
4.	Analysis	54
C.	GROUND 1C – Claim 4 is obvious over Smith in view of Kobylkin, Gomez, Saarisalo, and Slonecker	55
1.	Overview of Slonecker.....	55
2.	The combination of Smith, Kobylkin, Gomez, Saarisalo, and Slonecker	55
3.	Reasons to combine Smith, Kobylkin, Gomez, Saarisalo, and Slonecker	55
4.	Analysis	57
D.	GROUND 1D – Claims 5, 11, and 17 are obvious over Smith in view of Kobylkin, Gomez, and Mestre.....	58
1.	Overview of Mestre.....	58
2.	The combination of Smith, Kobylkin, Gomez, and Mestre	60

3.	Reasons to combine Smith, Kobylkin, Gomez, and Mestre	61
4.	Analysis	63
E.	GROUND 1E – Claim 6 is obvious over Smith in view of Kobylkin, Gomez, and Sahota	67
1.	Overview of Sahota	67
2.	The combination of Smith, Kobylkin, Gomez, and Sahota	68
3.	Reasons to combine Smith, Kobylkin, Gomez, and Sahota.....	69
4.	Analysis	71
F.	GROUND 1F – Claim 19 is obvious over Smith in view of Kobylkin, Gomez, and Moosavi	75
1.	Overview of Moosavi.....	75
2.	The combination of Smith, Kobylkin, Gomez, and Moosavi	76
3.	Reasons to combine Smith, Kobylkin, Gomez, and Moosavi	76
4.	Analysis	78
G.	GROUND 1G – Claims 20-27 are obvious over Smith in view of Kobylkin, Gomez, and Mullen	79
1.	Overview of Mullen	79
2.	The combination of Smith, Kobylkin, Gomez, and Mullen.....	79
3.	Reasons to combine Smith, Kobylkin, Gomez, and Mullen.....	80
4.	Analysis	81
IV.	DISCRETIONARY CONSIDERATIONS	88
V.	CONCLUSION AND FEES	90
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	91
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	91
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	91
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	91
D.	Service Information	92

EXHIBITS

SAMSUNG-1001	U.S. Patent No. 11,328,286 to Wyatt (“the ’286 patent”)
SAMSUNG-1002	Excerpts from the Prosecution History of the ’286 patent (“the Prosecution History”)
SAMSUNG-1003	Declaration and Curriculum Vitae of Dr. Michael Shamos
SAMSUNG-1004	U.S. Pub. No. 2013/0232083 (“Smith”)
SAMSUNG-1005	U.S. Pub. No. 2013/0166441 (“Kobylkin”)
SAMSUNG-1006	U.S. Pub. No. 2005/0043997 (“Sahota”)
SAMSUNG-1007	PCT Pub. No. 2012/154915 (“Mullen”)
SAMSUNG-1008	U.S. Pub. No. 2011/0078031 (“Mardikar”)
SAMSUNG-1009	U.S. Pub. No. 2011/0173121 (“Kawan”)
SAMSUNG-1010	U.S. Pub. No. 2011/0112918 (“Mestre”)
SAMSUNG-1011	U.S. Pub. No. 2009/0291634 (“Saarisalo”)
SAMSUNG-1012	U.S. Prov. No. 61/794,891 (“the ’286 provisional”)
SAMSUNG-1013	U.S. Pub. No. 2007/0045403 (“Slonecker”)
SAMSUNG-1014	U.S. Pub. No. 2008/0302876 (“Mullen-876”)
SAMSUNG-1015	PCT Pub. No. 2010/037218 (“Moosavi”)
SAMSUNG-1016	U.S. Pub. No. 2011/0173060 (“Gallagher”)
SAMSUNG-1017	U.S. Patent No. 9,600,808 (“Gomez”)
SAMSUNG-1018	PCI Data Security Standard (PCI DSS) Version 2.0 January 2013

- SAMSUNG-1019 Payment Card Industry (PCI) Data Security Standard
Navigating PCI DSS Version 2.0 October 2010
- SAMSUNG-1020 Kadambi et al., *Near-Field Communication-Based Secure
Mobile Payment Service*, ACM Proceedings of the 11th
International Conference on Electronic Commerce in August
2009 (“Kadambi”)
- SAMSUNG-1021—1099 [RESERVED]
- SAMSUNG-1100 Complaint for Patent Infringement, *Cardware Inc. v.
Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-cv-
00141 (E.D. Tex. May 11, 2022)
- SAMSUNG-1101 Interim Procedure for Discretionary Denials in AIA Post-
Grant Proceedings with Parallel District Court Litigation
(June 21, 2022)
- SAMSUNG-1102 Exhibit E to CardWare Inc.’s P.R. 3-1 Disclosure of
Asserted Claims and Infringement Contentions, *Cardware
Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-
cv-00141 (E.D. Tex. (Sept. 8, 2022)
- SAMSUNG-1103 United States District Courts National Judicial Caseload
Profile, *available at*
[https://www.uscourts.gov/sites/default/files/fcms_na_distpro
file0630.2022_0.pdf](https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0630.2022_0.pdf) (retrieved November 11, 2022)
- SAMSUNG-1104 Sample Docket Control Order for Patent Cases, *Cardware
Inc. v. Samsung Electronics Co., Ltd. et al.*, Case No. 2:22-
cv-00141 (E.D. Tex.)
- SAMSUNG-1105 Plaintiff CardWare Inc.’s Disclosure of Asserted Claims and
Infringement Contentions, *Cardware Inc. v. Samsung
Electronics Co., Ltd. et al.*, Case No. 2:22-cv-00141 (E.D.
Tex. (Sept. 8, 2022)

CLAIM LISTING

Limitation	Claim language
[1.0]	A payment system comprising:
[1.1]	a payment card device free of any fixed payment numbers visible thereon and wherein said payment card device is operable for use in payment card reader equipment; and
[1.2]	a computing device comprising a processor;
[1.3]	a memory;
[1.4]	a wireless interface;
[1.5]	a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and
[1.6]	a user-input device coupled to the processor, and
[1.7a]	wherein the processor is operable to store a transaction sequence count
[1.7b]	a device account number and
[1.7c]	secrets limited to the computing device, and
[1.8]	wherein the computing device is operable to receive, store and transmit a card payment information not visible on the payment card device, and
[1.9]	wherein the processor is operable to generate at least a portion of a limited-use card payment information for use by an authenticated card user, and
[1.10]	wherein the computing device is operable to convey said limited-use card payment information via an interface of the computing device, and
[1.11]	wherein a card issuer authority is operable to reject as invalid a transaction attempt outside of its limitations of use,
[1.12]	wherein a card issuer authority is operable to validate a card payment information as authentic when received from at least one of an authenticated users payment card; and an authenticated users computing device
[1.13]	and wherein the card issuer authority is operable to permit the authentic transactions to complete.
[2.0]	The system of claim 1, wherein the touch-screen user interface is operable to control an access for payment transactions by the card device, and is operable to enable as authentic payment transactions by the card device.
[7.0]	The system of claim 1, wherein the computing device is further operable to transceive the card payment information via the wireless interface for completing an online transaction.

[8.0]	The system of claim 1, wherein the computing device is further operable to transceive the limited-use card payment information via an NFC interface of the computing device in an in-store NFC reader facility transaction.
[9.0]	The system of claim 1, wherein the computing device is further operable to transceive the limited-use payment information wirelessly with another device via a wireless interface of the computing device, in a device-to-device transaction.
[10.0]	The system of claim 1, wherein the computing device is further operable to transmit a payment information visually, in alphanumeric, graphical and iconography via the touch screen user interface.
[12.0]	The system of claim 1, wherein the computing device is further operable to present at least one challenge, of a set of security challenges comprising: a card user personal information question, a card issuer authority security question, a user touch-screen entry, a user touch-screen swipe, a user gesture of a device, a user passcode entry, a biometric sensing of a user touch, a biometric sensing of a recognized user proximity, and a biometric sensing of a recognized user, and
[12.1]	wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and
[12.2]	wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user, and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least one challenge.
[13.0]	The user computing device of claim 12, wherein a payment issuing authority is operable to decline transactions performed by the computing device when a user fails the at least one security challenge.
[14.0]	The system of claim 1, wherein a payment issuing authority is operable to decline transactions performed by the payment card device when a user fails at least one security challenge presented to a user by the computing device.
[15.0]	A payment system comprising:
[15.1]	a payment card device that is free of any fixed payment numbers disposed thereon and wherein said payment card device is operable for use in a merchant card-reader equipment; and
[15.2]	a card-users personal computing device operable for completing a payment transaction and comprising a processor;
[15.3]	a touch-screen display interface;
[15.4]	a user-interface;
[15.5]	a wireless interface; and
[15.6]	a memory for storing a payment information accessible to the processor,

[15.7]	wherein the computing device is configured to dynamically generate limited-use payment information, and
[15.8]	wherein the computing device is configured to convey the limited-use payment information on a computing device interface upon the authorization of a valid user, and
[15.9]	wherein a merchant is operable to receive a payment information provided by a personal computing device, and
[15.10]	wherein the limited-use payment information provided by at least one or both of the payment card device, and the computing device, is validated by a card issuing authority when used in merchant in-store facility transactions, and
[15.11]	wherein a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use, and
[15.12]	wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.
[16.0]	The system of claim 15, wherein the touch-screen user interface is operable for displaying the limited-use payment information, and
[16.1]	wherein a merchant is operable to accept the displayed payment card information in a transaction at a merchant facility.
[18.0]	The system of claim 15, wherein a plurality of issuer-provided payment information is wirelessly downloaded into the personal computing device, and
[18.1]	wherein the user-interface is operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface, and
[18.2]	wherein the payment card device is operable for a transaction with a user-selected payment method.
[3.0]	The system of claim 1, wherein the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device.
[4.0]	The system of claim 3, wherein the touch-screen user-interface is configurable for a locking and unlocking of payment transactions, and wherein a card issuer authority is further operable for denying a payment transaction from at least one of: a locked card device; and a locked card-users computing device, and
[4.1]	wherein a card issuer authority is further operable to permit as authorized, a card payment transaction from an unlocked device.
[5.0]	The system of claim 1, wherein the payment card device is absent a payment number information necessary for completing an online transaction, and
[5.1]	wherein the information presented on an interface of said card device, are limited to an in-store merchant card reader facility use only.

[11.0]	The system of claim 1, further comprising a touch-screen user interface control for a user approving and denying a transaction, and
[11.1]	wherein a card issuer authority is further operable to deny as authentic, a card payment transaction from a user-denied transaction, and to approve as authentic a card payment transaction from a user-approved transaction.
[17.0]	The system of claim 15, wherein the touch-screen display interface is operable to display a merchant facility transaction, and
[17.1]	wherein the touch-screen display interface is operable to accept a user approval and denial of a payment transaction, and
[17.2]	wherein a card issuer authority is further operable to deny a card payment transaction from a user-denied merchant facility transaction, and to approve as authentic a card payment transaction from a user-approved facility transaction.
[6.0]	A system of claim 1, wherein: the card issuer authority is operable to receive said transacted payment information, and
[6.1]	wherein a card issuer authority is operable to compute a limited-use payment information from a transaction information, a merchant, a facility information, a sequence counter, a payment card account information, secrets and an information limited to said card device and to said computing device, and
[6.2]	wherein a card issuer authority is operable to compare said computed payment information to said device transacted information, and
[6.3]	wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations, and
[6.4]	wherein a card issuer authority is operable to authenticate as valid, a device transaction use within valid range of device limitations.
[19.0]	The card device of claim 15, wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and
[19.1]	wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.
[20.0]	A payment system comprising:
[20.1]	a payment card device, free of any depictions of fixed payment numbers thereon, and operable for use in payment card reader equipment; and
[20.2]	a computing device comprising a processor;
[20.3]	a memory;
[20.4]	a wireless interface;
[20.5]	a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and

[20.6]	a user-input device coupled to the processor; and
[20.7]	wherein the memory is operable to store a transaction sequence count, a static device account number and secrets limited to the computing device;
[20.8]	wherein the computing device is operable to receive, store, display and transmit issuer-provided payment information, associated with, but not depicted on, the payment card device;
[20.9a]	wherein the processor is operable to dynamically generate at least a portion of a limited-use payment information for use by an authenticated card user, and
[20.9b]	to combine said at least a portion of the limited-use payment information with at least said static device account number to create combined payment information;
[20.10]	wherein the computing device is operable to convey said combined payment information via an interface of the computing device; and
[20.11]	wherein the computing device is operable to receive information, from an issuer, in response to the conveyed combined payment information, indicating that a payment transaction is valid.
[21.0]	The system of claim 20 wherein the computing device is operable to wirelessly receive the static device account number.
[22.0]	The system of claim 20, wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information based on a transaction sequence counter count, and
[22.1]	further wherein the generated limited-use payment information is valid for a single use.
[23.0]	The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on payment processing authority secrets.
[24.0]	The system of claim 23 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.
[25.0]	The system of claim 24 wherein the computing device is operable to wirelessly receive the static device account number.
[26.0]	The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.
[27.0]	The system of claim 26 wherein the computing device is operable to wirelessly receive the static device account number.

Samsung Electronics Co., Ltd. (“Petitioner” or “Samsung”) petitions for Post Grant Review (“PGR”) of claims 1-27 (“the Challenged Claims”) of U.S. Patent No. 11,328,286 (“the ’286 patent”).

I. REQUIREMENTS FOR PGR

A. Grounds for Standing

The present Petition is being filed within one year of service of a complaint against Samsung alleging infringement of the ’286 patent. SAMSUNG-1100. Samsung is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

In addition, Petitioner certifies that the ’286 patent is available for PGR. In particular, the present Petition is being filed less than 9 months after the issue date of the ’286 patent (May 10, 2022). 35 U.S.C. § 321(c). In addition, the ’286 patent is an AIA patent that is eligible for PGR, as explained below.

B. The ’286 patent is an AIA patent and therefore eligible for PGR

In order to be eligible for PGR, the ’286 patent must be subject to the first-inventor-to-file provisions of the AIA. *Leahy-Smith America Invents Act*, Pub. L. No. 112–29, 125 Stat. 284 (September 16, 2011) (“AIA”), §6(f)(2)(A); *Tricam v. Little Giant Ladder*, PGR2021-00044, Paper 10 p. 14 (PTAB August 3, 2021) (“*Tricam*”). In order to be subject to the first-inventor-to-file provisions of the

AIA, Petitioner must show that the '286 patent contains or contained at any time "a claim that lacks written description and enabling support in a priority application filed before March 16, 2013." *Tricam*, 15. As discussed below, multiple claims of the '286 patent lack such support. The '286 patent is thus subject to the first-inventor-to-file provisions of the AIA, and therefore eligible for PGR. *See id.*

The '286 patent claims priority, through a string of continuations, to U.S. Provisional App. No. 61/794,891 (SAMSUNG-1012, the "'286 provisional"), which was filed March 15, 2013. But the '286 provisional does not disclose or otherwise reasonably convey at least the claim features listed in the table below. SAMSUNG-1003, [33].

Claim	Unsupported Language
3	"The system of claim 1, wherein the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device."
5	"The system of claim 1, wherein the payment card device is absent a payment number information necessary for completing an online transaction, and wherein the information presented on an interface of said card device, are limited to an in-store merchant card reader facility use only."
6	"A system of claim 1, wherein: the card issuer authority is operable to receive said transacted payment information, and wherein a card issuer authority is operable to compute a limited-use payment information from a transaction information, a merchant, a facility information, a sequence counter, a payment card account information, secrets and an information limited to said card device and to said computing device, and wherein a card issuer authority is operable to compare said computed payment information to said device transacted information,

Claim	Unsupported Language
	and wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations, and wherein a card issuer authority is operable to authenticate as valid, a device transaction use within valid range of device limitations.”
12	“The system of claim 1, wherein the computing device is further operable to present at least one challenge, of a set of security challenges comprising: a card user personal information question, a card issuer authority security question, a user touch-screen entry, a user touch-screen swipe, a user gesture of a device, a user passcode entry, a biometric sensing of a user touch, a biometric sensing of a recognized user proximity, and a biometric sensing of a recognized user, and wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user, and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least one challenge.”
15	“wherein a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use, and wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.”
20	“wherein the computing device is operable to receive, store, <i>display</i> and transmit issuer-provided payment information, associated with, but not depicted on, the payment card device.”

For example, with respect to claim 3, the provisional application briefly mentions that “[o]ne type of credit card in circulation employs radio frequency (“RF”) identification where there is a near field radio frequency.” SAMSUNG-1012, [0004]. The provisional application later describes that “the card could use RFID or near field technology so that it can connect to a personal computer and be

used to uniquely generate a credit card number for online purchases.” *Id.*, [0017].

There is no other discussion of near field communication or “NFC” in the provisional application. Claim 3’s recitation of “the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device” is therefore not supported by the provisional application. SAMSUNG-1003, [34]. Additionally, there is no disclosure in the provisional application of using touch-screen input to control enabling or disabling of any payment transaction functionality regardless of the communication method used. SAMSUNG-1003, [34].

As another example, the provisional application does not describe limiting the field of use of the payment card device to in-store card reader facility use only, to the exclusion of online transactions and therefore lacks support for claim 5. SAMSUNG-1003, [35]. Rather than limiting the use to in-store transactions to the exclusion of online transactions, the provisional application states, “the credit card of the present invention could also be used to make online purchases.” SAMSUNG-1012, [0017].

Regarding claim 6, the provisional application includes a single discussion of “wherein the time, sequence, user, credit card authority and other information is similarly combined by credit card processing facility to generate a credit card

number for comparison to the number transmitted by the credit card reader.”

SAMSUNG-1012, claim 6. The provisional does not provide support for challenged claim 6 because it does not disclose generating a limited-use number “from a transaction information, *a merchant*, a *facility information*, a sequence counter, a payment card account information, secrets and an information *limited to said card device and to said computing device*.” SAMSUNG-1003, [36]. There is also no disclosure of “wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations, and wherein a card issuer authority is operable to authenticate as valid, a device transaction use within valid range of device limitations” as recited by challenged claim 6. SAMSUNG-1003, [36].

With respect to claim 12, the provisional application describes “ask[ing] the user a security question if an improper password is entered” but does not provide support for all of the “security challenges” recited by claim 12. SAMSUNG-1003, [37]. There is also no disclosure in the ’286 Provisional of “wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user, and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least

one challenge.” The provisional application describes a security question being presented “if an improper password is entered” but does provide details on actions performed in response to a correct or incorrect answer to the security question. SAMSUNG-1003, [37].

There is also no support for claim 15’s recitation of “a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use.” The provisional briefly mentions that a “credit card processing facility” authenticates the transaction but does not describe the “credit card processing facility” as being a card issuing authority or as performing the precise functionality recited by Elements 15.11 and 15.12.

The ’286 provisional thus does not provide support for at least these claims of the ’286 patent. No other application in the priority chain of the ’286 patent was filed prior to March, 16, 2013. Accordingly, at least the claims listed above “lack[] written description and enabling support in a priority application filed before March 16, 2013.” *Tricam*, 15. The ’286 patent is thus subject to the first-inventor-to-file provisions of the AIA, and is therefore eligible for PGR. *See id.*

C. Challenge and Relief Requested

Samsung requests a PGR of the Challenged Claims on the grounds noted below. Dr. Michael Shamos provides supporting testimony in his Declaration. SAMSUNG-1003, [84]-[378].

Ground	Claim(s)	35 U.S.C. §103
1A	1, 2, 7-10, 12-16, 18	Obvious over Smith in view of Kobylkin, and Gomez
1B	3	Obvious over Smith in view of Kobylkin, Gomez, and Saarisalo
1C	4	Obvious over Smith in view of Kobylkin, Gomez, Saarisalo, and Slonecker
1D	5, 11, 17	Obvious over Smith in view of Kobylkin, Gomez, and Mestre
1E	6	Obvious over Smith in view of Kobylkin, Gomez, and Sahota
1F	19	Obvious over Smith in view of Kobylkin, Gomez, and Moosavi
1G	20-27	Obvious over Smith in view of Kobylkin, Gomez, and Mullen

The earliest claimed priority date of the '286 patent is March 15, 2013 (hereinafter the "Critical Date"). Each of the prior art references applied in the above-listed Grounds qualifies as prior art to the '286 patent as shown below:

Reference	Dates	Prior Art Basis
Smith	March 1, 2013 (filed) March 1, 2012 (priority)	35 U.S.C. § 102(a)(2)
Kobylkin	Dec. 21, 2012 (filed) Dec. 22, 2011 (priority)	35 U.S.C. § 102(a)(2)
Sahota	Feb. 24, 2005 (published)	35 U.S.C. § 102(a)(1)
Mullen	Nov. 15, 2012 (published)	35 U.S.C. § 102(a)(2)
Mestre	May 12, 2011 (published)	35 U.S.C. § 102(a)(1)
Saarisalo	Nov. 26, 2009 (published)	35 U.S.C. § 102(a)(1)
Slonecker	Mar. 1, 2007 (published)	35 U.S.C. § 102(a)(1)
Gomez	Jun. 22, 2012 (published)	35 U.S.C. § 102(a)(1)

Reference	Dates	Prior Art Basis
Moosavi	Apr. 10, 2010 (published)	35 U.S.C. § 102(a)(1)

None of these references were considered during prosecution of the '286 patent.

D. Claim Construction

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. Besides the specific constructions described below, no formal claim constructions are presently necessary since “claim terms need only be construed to the extent necessary to resolve the controversy.” *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011); SAMSUNG-1003, [80]-[83].

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board in accordance with due process. Furthermore, Petitioner does not concede that the Challenged Claims satisfy all statutory requirements, including those under 35 U.S.C. §§ 101 and 112.

1. Claim limitations directed to printed matter are not entitled to patentable weight (claims 1, 5, 15, 19, 20)

The Challenged Claims include several limitations that are directed to printed matter that has no functional or structural relationship to the claimed substrate on which the information is disposed or printed. The Federal Circuit has

repeatedly found that such claim limitations are entitled to no patentable weight, and thus “will not distinguish the invention from the prior art in terms of patentability.” *In re Gulack*, 703 F. 2d 1381, 1385 (Fed. Cir. 1983); *see, e.g., In re DiStefano*, 808 F. 3d 845, 848-851 (Fed. Cir. 2015).

The following table identifies limitations from the Challenged Claims that are directed to printed matter, and thus are entitled to no patentable weight. As described in greater detail in Section III, regardless of whether these limitations are entitled to patentable weight, they are nonetheless rendered obvious by the references cited in the present Petition.

Claim	Language Representing Printed Matter
1	“free of any fixed payment numbers visible thereon” / “a card payment information not visible on the payment card device”
5	“wherein the payment card device is absent a payment number information necessary for completing an online transaction”
15	“free of any fixed payment numbers disposed thereon”
19	“wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.”
20	“free of any depictions of fixed payment numbers thereon”

2. Additional non-limiting claim features

The features recited in claim elements [1.12], [1.13], [6.0]-[6.4], [11.1],

[13.0], [14.0], [15.11], [15.12], and [17.2] are not limiting as they do not define further limitations of the recited payment devices and systems. For example, element [1.12] recites, in relevant part, “wherein a card issuer authority is operable to validate a card payment information as authentic[.]” But the “card issuer authority” in this claim element is not recited as being included in the “payment system” to which claim 1 is directed. Thus, the language describing a function the card issuer authority “is operable” to perform does not limit any aspect of the claimed payment system, and thus does not affect the scope of the claim.

These features are nonetheless obvious for the reasons described in further detail in Section III.

E. Level of Ordinary Skill in the Art

A person of ordinary skill in the art as of the Critical Date (a “POSITA”) would have had (1) a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) one to two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technologies. SAMSUNG-1003, [49]-[54]. Additional education could substitute for professional experience, or vice versa. *Id.*

II. THE ’286 PATENT

The ’286 patent specification generally describes an electronic payment card

capable of generating a “limited-duration number” for use in a payment transaction. SAMSUNG-1001, 2:33-39, 2:57-3:5, 10:63-12:55, FIG. 7; SAMSUNG-1003, [28]. Figure 7 depicts a flowchart of a process for generating and using a limited-duration number in a transaction:

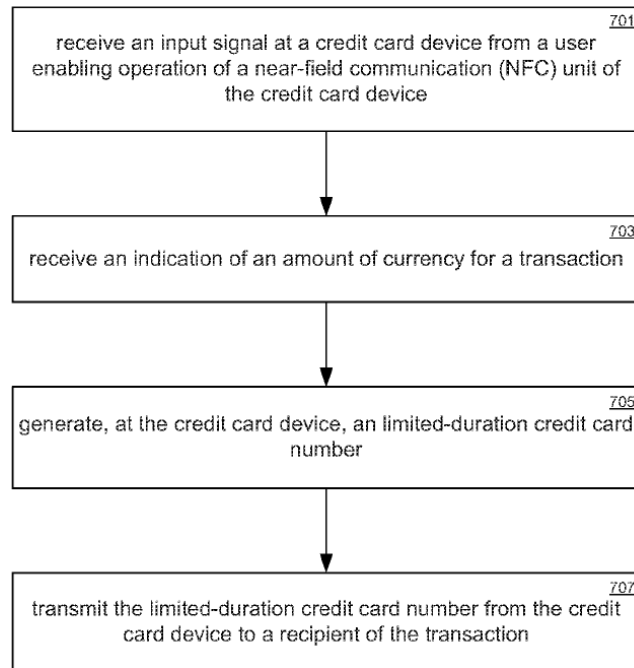


FIG. 7

SAMSUNG-1001, FIG. 7.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A – Claims 1, 2, 7-10, 12-16, and 18 are obvious over Smith in view of Kobylkin, and Gomez

1. Overview of Smith

Smith describes a payment system in which real card account numbers (RCAs) are mapped to mobile cloud account numbers (MCAs), and in which MCAs are used in conjunction with a generated cryptogram to facilitate payment

transactions over the standard credit card payment network. *See, e.g.*, SAMSUNG-1004, Abstract, [0029]-[0031], [0034], [0063]-[0065], FIG. 1. Smith describes that payment transactions in its system can be initiated from a “mobile device,... such as a cellular phone, smart phone, table computer, etc.” *See, e.g., id.*, [0033]. Smith describes that the mobile device wirelessly obtains “mobile cloud account data” when a “mobile cardlet” including the mobile cloud account data is provisioned “over-the-air (OTA)” to the mobile device. *Id.*, [0044]. Smith describes that the mobile device “generat[es]...a payment cryptogram based on at least a portion of the mobile cloud account data 802” each time a payment transaction is initiated. *Id.*, [0103]. Smith describes that the “payment cryptogram” is transmitted to a “service provider,” where it is used to “validate” the payment transaction. *Id.*, [0096], [0097].

2. Overview of Kobylkin

Kobylkin describes an “instant disposable payment card” having a “magnetic strip” containing a “code” that can be “scanned” or “read” by a merchant to “facilitate payment for [a] purchase.” SAMSUNG-1005, [0015]. “For example, the merchant can ... swipe a magnetic strip of the payment card to facilitate payment for the purchase.” *Id.*

Kobylkin further describes that the payment card “can be a substantially blank card” lacking “any information” printed or disposed thereon. *Id.*, [0017].

Kobylkin teaches that selected information can be printed on the card, such as a “company name and/or logo of the provider,” “the user’s name,” or “any desired information.” *Id.*, [0018].

3. Overview of Gomez

Gomez describes that a “payment card system uses a static payment card identifying number and generates, for each attempted transaction, an authentication cryptogram based at least upon a seed value stored within the payment card and further based upon a temporal signal value that changes for each attempted use of the payment card.” SAMSUNG-1017, Abstract. Gomez describes a device that “generates an authentication cryptogram for each attempted transaction only after the cardholder successfully presents a credential, such as a fingerprint or PIN number, into the payment card” (i.e., after a user input approving the transaction). SAMSUNG-1017, 5:14-18.

Gomez further discloses how a cryptogram for a transaction can be displayed on a device. SAMSUNG-1017, 13:1-4 (“cryptogram may be displayed”), 14:3-7.

4. The combination of Smith, Kobylkin, and Gomez

In the present combination, the mobile device utilized in Smith’s online payment system is adapted to be used for the additional and independent purpose of activating and/or funding a disposable payment card like that described in

Kobylkin. SAMSUNG-1005, [0031] (“The user can activate or fund the instant disposable payment card ... with the user’s smart phone”), [0072]; *see also id.*, [0039], [0041], [0052], [0084], [0134]. For example, the modified mobile device in the combination would be configured to read a card account number from the disposable card by bringing the phone in close proximity to the card for an NFC-based communication or by scanning a QR code printed on the card. *Id.*, [0050], [0070], [0085]. Activation or funding of the disposable payment card would then proceed using Smith’s mobile device in substantially the same manner described in Kobylkin. SAMSUNG-1003, [117].

Further, in the combination, Smith’s payment cards can be implemented as “substantially blank card[s]” with only selected, non-confidential information, such as a “company name and/or logo of the provider,” printed or disposed thereon, based on the teachings of Kobylkin. SAMSUNG-1003, [118]; *see, e.g.*, SAMSUNG-1004, [0031]; SAMSUNG-1005, [0015]-[0018].

In addition, in the combination, the payment device of Smith stores a transaction sequence count based on the teachings of Gomez. SAMSUNG-1017, 7:24-26, 8:37-41, 10:34-42, FIG. 7; *see also* 10:66-11:2; SAMSUNG-1003, [119]. Also in the combination, the payment device of Smith “generates an authentication cryptogram for each attempted transaction” based on the teachings of Gomez. SAMSUNG-1017, 5:25-28. Further, in the combination, Smith’s cryptogram is

generated “only after the cardholder successfully presents a credential, such as a fingerprint or PIN number, into the payment card,” based on the teachings of Gomez. *Id.*; SAMSUNG-1003, [119].

5. Reasons to combine Smith, Kobylkin, and Gomez

Combining Smith and Kobylkin

A POSITA would have found it obvious and would have been motivated by multiple reasons to extend the functionality of Smith’s mobile device for use in activating and/or funding a disposable payment card as taught in Kobylkin. SAMSUNG-1003, [120]. Indeed, a POSITA would have found that adapting Smith’s mobile device in this manner would have been beneficial to allow a user to make ready use of disposable payment cards. *Id.* Kobylkin expressly describes a number of desirable properties of disposable payment cards that would have motivated their use in the combination, including that they can be “disposable and easily made”; the disposable cards “have no value to anyone unless and when the user funds” the cards; funding of the disposable cards “can be easily accomplished anywhere by the user ... with a user smart phone”; and the disposable cards “provide a safe way for the user to make payments, while limiting exposure that a credit or debit card can have.” SAMSUNG-1005, [0052].

Moreover, adapting Smith’s mobile device to fund and/or activate disposable cards according to Kobylkin’s funding and/or activation techniques

would have been obvious considering that ordinary mobile devices (*e.g.*, smartphones of the same or similar character to those described in Smith) were well suited to facilitate these funding and/or activation processes, as taught in Kobylkin. SAMSUNG-1004, [0033], [0004] (“NFC-capable mobile devices”); SAMSUNG-1005, [0031], [0050] (“user’s device has an NFC reader”), [0052] (“user smart phone”), [0134]. To be sure, as of the Critical Date of the ’286 patent, smartphones were commonly configured to host multiple applications that would allow a user to perform a range of tasks or activities (*e.g.*, check email, play games, capture photos and videos, play media files, browse the web, make payments, and more). SAMSUNG-1003, [121]. In this context, a POSITA would have desired to permit a user to perform Kobylkin’s activation and funding operations on the *same* mobile device as the user uses for other tasks such as conducting mobile payment transactions as taught in Smith—especially since use of the same device for both purposes would have increased convenience and freed the user from needing to access separate devices for performing online payment transactions based on Smith’s techniques and for funding or activating a disposable card based on Kobylkin’s. *Id.*

Further, a POSITA would have found it obvious to adapt Smith’s mobile device to be used in funding and/or activating a disposable card based on Kobylkin because doing so entails the mere use of known solutions to improve similar

systems and methods in the same way. SAMSUNG-1003, [122]. “[W]hen a patent ‘simply arranges old elements with each performing the same function it had been known to perform’ and yields no more than one would expect from such an arrangement, the combination is obvious.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Kobylkin’s teachings to Smith as described above would have led to predictable results without significantly altering or hindering the functions performed by Smith’s mobile device. SAMSUNG-1003, [122]. A POSITA would have had a reasonable expectation of success adapting Smith’s mobile device to activate and/or fund a disposable payment card like that described in Kobylkin in light of the fact that similar mobile devices are described for performing the respective operations in Smith’s online payment system and Kobylkin’s disposable payment card system. *Id.*

A POSITA next would have been motivated and found it obvious to modify the payment cards in Smith’s payment system (e.g., the physical payment cards corresponding to virtual cardlets with MCAs stored in the mobile device) to include only selected, non-confidential information on its face, as described in Kobylkin. SAMSUNG-1003, [123]. A POSITA would have understood that the payment cards of Smith would present less risk of fraud if confidential payment information, such as a static security code or other non-changing portion of the

payment information, were not readily ascertainable simply by visually inspecting the face of the dynamic credit card. SAMSUNG-1003, [123]; *see, e.g.*, SAMSUNG-1012, [0003] (“A thief may, for example, catch a glimpse of an actual credit card and copy the number by writing the number on a piece of paper.”); SAMSUNG-1005, [0006].

Further, a POSITA would have found it obvious to modify Smith’s payment cards based on Kobylkin’s teachings because doing so entails the mere use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [124]. *KSR*, 550 U.S. at 417. A POSITA would have recognized that applying Kobylkin’s teachings to Smith would have led to predictable results without significantly altering or hindering the functions performed by Smith’s system. SAMSUNG-1003, [124].

Accordingly, for at least these reasons, augmenting Smith’s device based on the teachings of Kobylkin would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

Combining Smith and Gomez

A POSITA would have been motivated and found it obvious for Smith’s payment device to store a transaction sequence count, and to generate a payment cryptogram for each transaction only after receiving a valid credential (*e.g.*, a PIN)

from the user, based on the teachings of Gomez. SAMSUNG-1003, [126]. Smith describes one of its aims as “reducing the potential for fraud” in payment transactions performed by its system. SAMSUNG-1004, [0034]. Although Smith describes many mechanisms for securing the various sensitive information transferred between and stored by the components of its system, it focuses less on preventing fraud stemming from unauthorized use of the mobile device. *See, e.g., id.*, [0045] (describing a user merely selecting an MCA on the mobile device to initiate a payment transaction); SAMSUNG-1003, [126]. Implementing Gomez’s transaction counting and cryptogram generation techniques in Smith’s mobile device would further Smith’s aim of “reducing the potential for fraud” by preventing the use of a stolen mobile device to initiate fraudulent transactions, and preventing the re-use of intercepted cryptograms for additional transactions, as taught by Gomez. SAMSUNG-1004, [0034], [0045]; SAMSUNG-1017, 5:39-41, 7:24-26, 8:37-41, 10:34-42, 10:66-11:2, FIG. 7; SAMSUNG-1003, [126].

In addition, it would have been obvious to modify Smith’s mobile device so that the payment cryptogram would be displayable on a display of the device, as taught in Gomez. SAMSUNG-1003, [127]. A POSITA would have been motivated to integrate Gomez’s teaching for displaying a payment cryptogram in the mobile device of the combination to facilitate online transactions, as expressly taught in Gomez. SAMSUNG-1017, 13:1-4 (“beneficial in facilitating an online

transaction”), 14:1-7 (communicating the cryptogram “using an online web page”).

For example, displaying the cryptogram would allow a user to input the cryptogram into an online form for an online transaction when the cryptogram is not communicated through a card reader NFC interface. *See id.*; SAMSUNG-1003, [127]. A POSITA would have had a reasonable expectation of success implementing the combination since the mobile device in the combination has a display capable of displaying numbers, and the device generates the cryptogram locally such that it could be readily displayed. *Id.*

Further, a POSITA would have found it obvious to modify Smith’s mobile device based on Gomez’s teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [128]. Here, “when a patent ‘simply arranges old elements with each performing the same function it had been known to perform’ and yields no more than one would expect from such an arrangement, the combination is obvious.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Gomez’s teachings to augment Smith’s mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith’s mobile device. SAMSUNG-1003, [128].

In fact, a POSITA would have been motivated to incorporate the well-known techniques of Gomez into Smith’s mobile device to achieve the predictable

benefits described in Gomez. SAMSUNG-1004, [0034], [0045]; SAMSUNG-1017, 5:39-41, 7:24-26, 8:37-41, 10:34-42, 10:66-11:2, FIG. 7; SAMSUNG-1003, [129].

Indeed, a POSITA would have had a reasonable expectation of success implementing Gomez's teachings in the context of Smith's mobile device, because Gomez implements its teachings in a device similar to Smith's. *See* SAMSUNG-1004, [0033]; SAMSUNG-1017, 5:39-41, 7:24-26, 8:37-41, 10:34-42, 10:66-11:2, FIG. 7; SAMSUNG-1003, [130].

Accordingly, for at least these reasons, augmenting Smith's mobile device based on the teachings of Gomez would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

6. Analysis

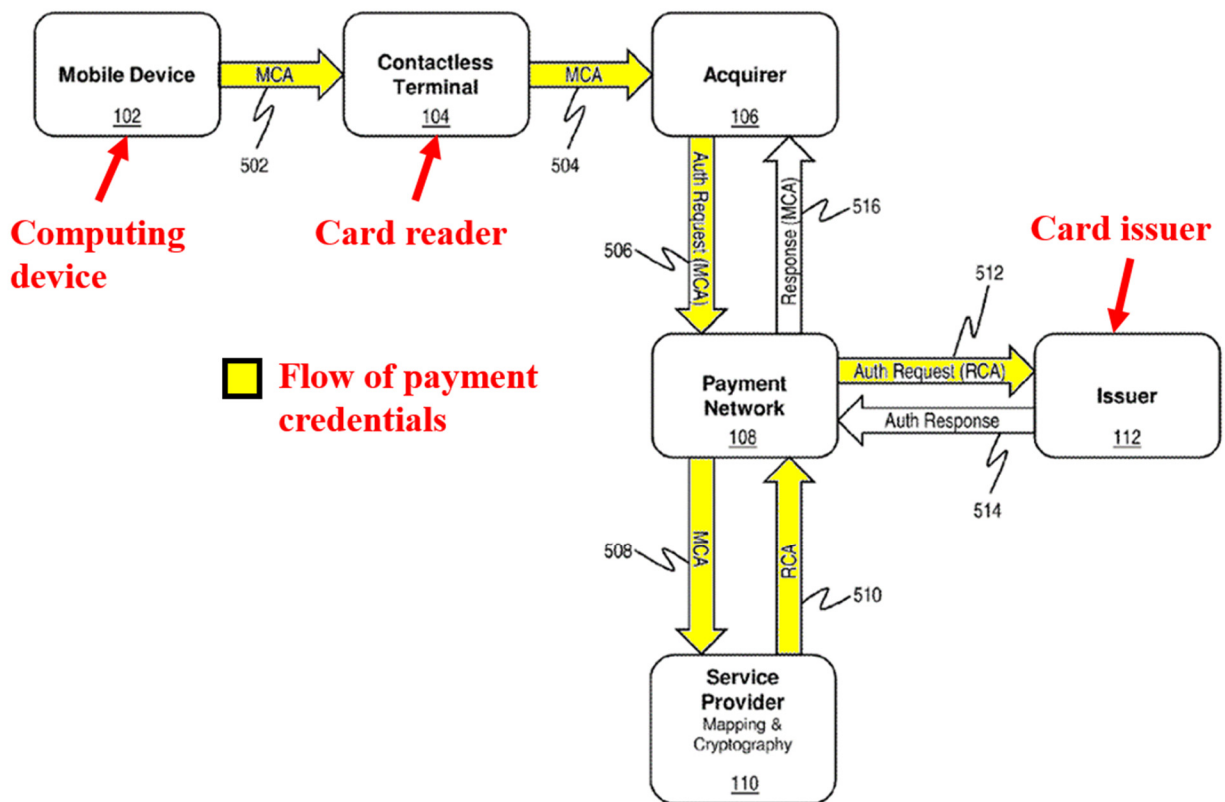
(a) Claim 1

Limitation [1.0]

In the combination, Smith describes a “***system for processing a financial transaction***” (*i.e.*, a payment system). SAMSUNG-1004, [0011].¹ As shown in FIG. 5 from Smith, reproduced below, the system includes “a mobile device 102,” that “transmit[s] payment credentials ... to a contactless point-of-sale terminal 104

¹ All emphasis added unless otherwise indicated.

via near field transaction.” *Id.*, [0033], [0035], FIG. 1, FIG. 5. The payment credentials are then processed and verified by various entities connected to a payment network 108 (e.g., the acquirer 106, and the issuer 112) to complete the transaction. *See id.*, [0036]-[0038]; SAMSUNG-1003, [132]. FIG. 5 shows this configuration:



SAMSUNG-1004, FIG. 5

Limitation [1.1]

In the combination, Kobylkin describes an “instant disposable ***payment card***” that can “be ***used as a point of sale (POS) debit or credit card***” (i.e.,

operable for use in payment card reader equipment). SAMSUNG-1005, [0024]; *see also* [0015] (user can “swipe a magnetic strip of the payment card to facilitate payment for [a] purchase.”); SAMSUNG-1003, [134].

In addition, as previously discussed (*see* Section I.C, *supra*), the limitation that the payment card device be “free of any fixed payment numbers visible thereon” is directed to printed matter (*i.e.*, the fixed payment numbers) that has no functional or structural relationship to the claimed card device, and thus is entitled to no patentable weight; SAMSUNG-1003, [135].

The combination renders the limitation obvious nonetheless. In the combination, Kobylkin further describes that the payment card “can be *a substantially blank card.*” *Id.*, [0017]. Kobylkin teaches that the card “*can lack any information ... thereon.*” *Id.* Thus, Kobylkin teaches that the payment card device is “free of any fixed payment numbers visible thereon.” *See id.*; SAMSUNG-1003, [136].

Limitation [1.2]

In the combination, Smith describes that its payment system includes a “*mobile device*” (*i.e.*, personal computing device) that can be “any type of mobile computing device... such as a cellular phone, smart phone, table computer, etc.” SAMSUNG-1004, [0033]. Smith further describes that the mobile device includes a “*processor.*” *See, e.g., id.*, [0042] (“The payment application 208 may be an

application program stored on the mobile device 102 and executed by a processor of the mobile device.”), [0104] (“mobile device ... may be implemented in the computer system 1300” shown in FIG. 13), [0108], FIG. 13; SAMSUNG-1003, [138].

Limitation [1.3]

In the combination, Smith describes that the mobile device includes memory. For example, Smith describes that the “mobile device ... may be implemented in the computer system 1300” shown in FIG. 13, which includes “a ***main memory*** 1308 (e.g., random access memory, read-only memory, etc.)” and “a ***secondary memory*** 1310.” SAMSUNG-1004, [0104], [0108]; SAMSUNG-1003, [140]. FIG. 13 from Smith shows these components of the mobile device:

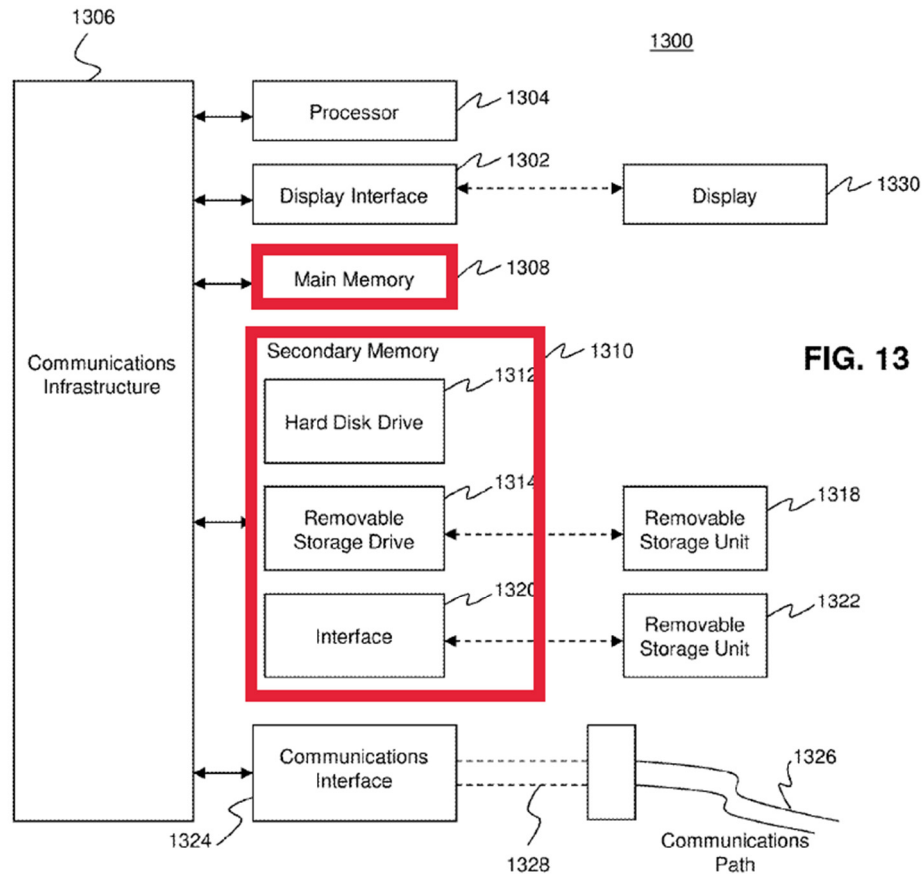


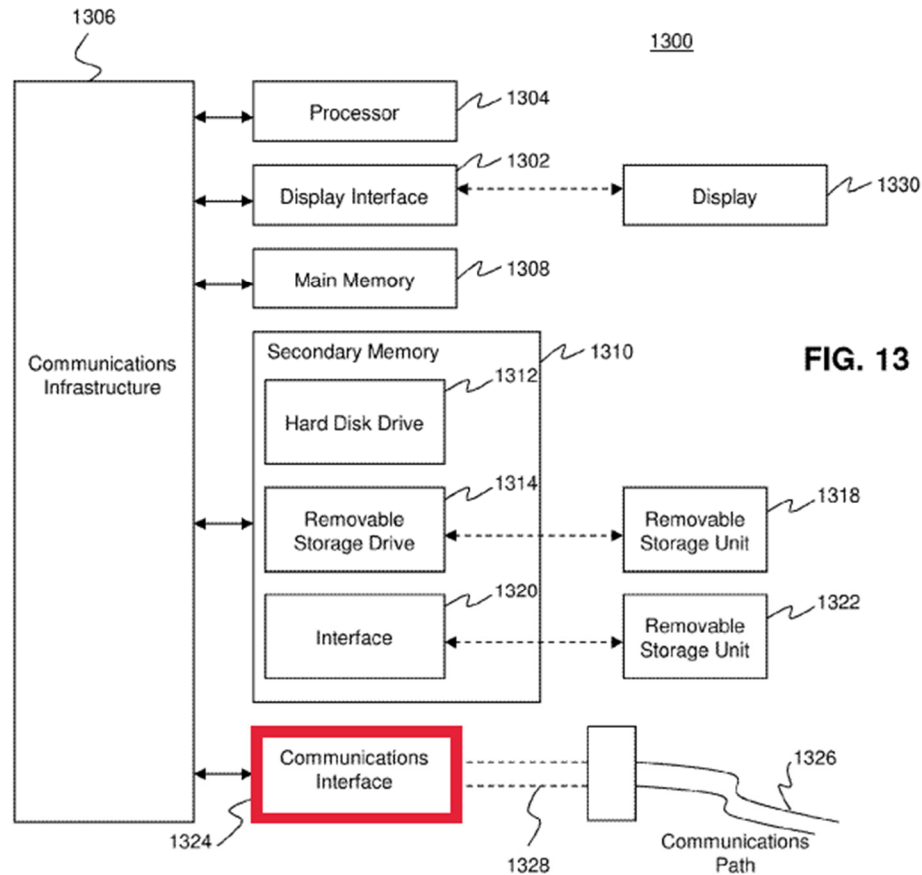
FIG. 13

SAMSUNG-1004, FIG. 13 (annotated)

Limitation [1.4]

In the combination, Smith describes that the “mobile device ... may be implemented in the computer system 1300” shown in FIG. 13, in which the “processor device 1304 may be connected to ... *a wireless network (e.g., WiFi)*, a mobile communication network, a satellite network” or a “radio frequency (RF)” network. SAMSUNG-1006, [0104], [0108]. Smith describes a “*communications interface 1324* ... configured to allow software and data to be transferred between

the computer system 1300” and these networks. *Id.*, [0112]; SAMSUNG-1003, [142]. FIG. 13 from Smith shows this component of the mobile device:



SAMSUNG-1004, FIG. 13 (annotated)

Limitation [1.5]

Smith describes that the mobile device (the computing device, *see* [1.2], *supra*) includes “***a payment user interface (UI)***” that is “***provided for the user for management of a payment application 208,***” which is “stored on the mobile device 102 and executed by a processor of the mobile device.” SAMSUNG-1004, [0042]. Smith describes that the mobile device “displays” information “via the

payment UI,” thereby indicating that the payment UI is a “visual user-interface.”

Id., [0055]. Smith describes that the user interacts with the “payment UI” via an “input device” such as a “***touch screen***” included in the mobile device. *Id.*, [0102]; SAMSUNG-1003, [144].

Limitation [1.6]

As described above (*see* [1.5], *supra*), in the combination, Smith describes that the user interacts with the “payment user interface” via an “***input device***” such as a “***touch screen***” included in the mobile device. SAMSUNG-1004, [0102]; SAMSUNG-1003, [146].

Limitation [1.7a]

In the combination, Gomez describes a “payment card” including a “processor” that stores a “sequence value (or sequential number)” (*i.e.*, a transaction sequence count) that is “increment[ed] for each attempted use” of the card. SAMSUNG-1017, 7:24-26, 8:37-41, 10:34-42, FIG. 7; *see also* 10:66-11:2; SAMSUNG-1003, [147]. As previously discussed, it would have been obvious to a POSITA for the payment device of Smith to store a transaction sequence count based on the teachings of Gomez. *See* Sections III.A.4-5, *supra*.

Limitation [1.7b]

First alternative mapping. In the combination, Smith teaches that the processor of the mobile device stores a “***mobile cloud account number (MCA)***” (*i.e.*, a device account number) “which may be associated with a real card account

number (RCA).” SAMSUNG-1004, [0034]. Smith describes that the “MCA may be mapped to the RCA such that *the user may conduct a financial transaction using the MCA for funding of the financial transaction*, and the funds may be supplied by the payment account corresponding to the RCA.” *Id.* “As a result,” Smith continues, “the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.” *Id.*; SAMSUNG-1003, [149].

Second alternative mapping. In the combination, Smith teaches that the processor of the mobile device stores a “*real card account number (RCA)*” for which the user can request to obtain a corresponding mobile cloud account number (MCA). SAMSUNG-1004, [0055]-[0056] (“In step 414, the MNO 304 may transmit the eligible RCAs to the mobile device 102, for display to the user 302 at step 416 (e.g., via the payment UI 204). ... In step **418**, the user **302** may request an MCA for a real card account.”), FIG. 4A. The processor of the mobile device further stores a portion of the “*real card account number (RCA)*” (*i.e.*, a device account number) as part of the mobile cloud account number (MCA). SAMSUNG-1004, [0083] (“[T]he MCA may include at least a portion of the RCA. In a further embodiment, the portion may be at least the last four digits of the RCA.”), [0095]; SAMSUNG-1003, [150].

Third alternative mapping. In the combination, Smith teaches that the

processor of the mobile device stores in a secure element an “*integrated circuit card (ICC) public key*” and an “*ICC private key*,” each of which comprises a number indicative of a device account of a user (*i.e.*, a device account number). SAMSUNG-1004, [0077], [0080]-[0081], [0089]-[0092]; SAMSUNG-1003, [151].

Limitation [1.7c]

Smith describes that the mobile device (*i.e.*, the computing device) includes a “secure element 210,” which is “a tamper-resistant platform, such as a hardware chip.” SAMSUNG-1004, [0043]. Smith describes that the “secure element 210 may store at least *a master key identifier* and *a mobile cardlet*.” *Id.*, [0043] (the “master key identifier [is] a value that is unique to the mobile device”), [0045] (the “mobile cardlet [is] configured to store mobile cloud account data for the transmission of payment credentials ... to the contactless terminal 104 for the conducting of a payment transaction”), [0056] (the master key identifier used by the service provider to authenticate the mobile device). A POSITA would have understood or at least found it obvious that items stored in a secure, tamper-resistant storage of a device—such as the master key identifier and a mobile cardlet stored in the secure element—are “secrets limited to the device.” SAMSUNG-1003, [153]; *see, e.g.*, SAMSUNG-1004, [0043]-[0045], [0056], FIG. 4A.

Limitation [1.8]

First alternative mapping

In the combination, the mobile device of Smith (*i.e.*, the computing device) is operable to receive, store, and transmit the card account number (*i.e.*, card payment information) of a disposable payment card like that described in Kobylkin, as discussed in [1.1], *supra*; SAMSUNG-1003, [155].

More specifically, Kobylkin describes that the payment card includes an “NFC code” or “RFID code” that encodes an “account number” for the card, and in the combination, Smith’s mobile device is used to fund and/or activate the card by a process that involves scanning the NFC or RFID code from the card as taught in Kobylkin. SAMSUNG-1005, [0137] (“As used herein, the term ‘scan’ can refer to any process for determining a code or other information, such as from the instant disposable payment card. Thus, scanning can include reading or imaging a QR code, a bar code, an SKU, an NFC code, and RFID code, or any other code.”), [0138] (“Although a QR code is referred to herein, such reference is by way of example only and not by way of limitation. A QR code, a bar code, an SKU, an NFC code, an RFID code, as well as any other code or combination of codes can be used.”), [0050] (“The user can also be able to load the instant disposable payment card using the NFC chip if the user's device has an NFC reader.”); [0031] (“The user can activate or fund the instant disposable payment card ... with the user’s smart phone”), [0072]; *see also id.*, [0039], [0041], [0052], [0084], [0134]; *supra*, Section III.A.5-6; SAMSUNG-1003, [156]. Thus, in the combination, when

the user scans the NFC or RFID code on the payment card of Kobylkin using the mobile device of Smith, the mobile device receives the account number of the payment card (*i.e.*, the card payment information). *Id.* Indeed, the mobile device subsequently transmits the card account number to a payment provider after scanning the card when activating or funding the card, and hence a POSITA would have understood that the mobile device receives the account number when the card is scanned. SAMSUNG-1005, [0031], [0072]; SAMSUNG-1003, [156].

Kobylkin also describes that the account number can alternatively be encoded in a “quick response (QR) code” printed on the payment card. SAMSUNG-1005, [0012], [0030]; [0023], [0040], [0046] (“The QR code can contain information about a merchant, a user, a user account, a payment provider, a code, stripe, or card identifier, or other desired information.”); [0070]. In the combination, the user scans the QR code on the payment card of Kobylkin using the mobile device (*e.g.*, smart phone) of Smith. *Id.*, [0012] (“The code can be scanned or otherwise read by the user, such as with a smart phone or other device.”), [0031] (“The card account number is encoded in the QR code.”); SAMSUNG-1004, [0033]. The account number encoded in the QR code would not be “visible” on payment card device, because it would not be apparent to a user viewing the QR code what account number it encodes. *Id.*, [0012]; SAMSUNG-1003, [157]. Thus, in the combination, when the user scans the QR code on the

payment card of Kobylkin using the mobile device of Smith, the mobile device would also receive the account number of the payment card (*i.e.*, the card payment information).

Also in the combination, Kobylkin describes how scanning the card causes the mobile device to “connect[] the user to the payment provider web site.” SAMSUNG-1005, [0031]. “The card account number is ... transferred to the payment provider over the communication link (URL encoded or tone dialing code).” *Id.*; *see also id.*, (additionally disclosing that “[t]he activation can take place completely manually via typing in or reading out over the phone.”), [0072] (“[T]he code can be scanned with the user’s mobile device and can be entered, either automatically or manually, into a form of the website.”), [0088]. Thus, in the combination, the mobile device of Smith transmits the card account number (*i.e.*, the card payment information) associated with the payment card of Kobylkin. SAMSUNG-1003, [158].

A POSITA would have understood or at least found obvious that the mobile device of Smith stores the card account number encoded in the QR code of Kobylkin (*i.e.*, the card payment information) for at least a period of time between receiving the card account number when the card is scanned and transmitting the card account number when the card is to be activated or funded. SAMSUNG-1003, [159]. In some examples, the mobile device would *store* the card account

number for at least a period of time that would permit the card account number to be displayed on the mobile device so that the user could manually enter the number into a form on a website. *Id.*, [0031] (“The activation can take place completely manually via typing in or reading out over the phone.”), [0072] (“[T]he code can be scanned with the user’s mobile device and can be entered, either automatically or manually, into a form of the website.”), [0088] (mobile device “app” for activating a disposable payment card). In further examples, Kobylkin describes how a disposable payment card can be “stored in the mobile device” along with “information ... to facilitate a purchase” with the payment card. *Id.*, [0087]. The card account number is used to access a funded account for making purchases, and a POSITA therefore would have understood or found obvious that the card account number is stored on the mobile device in these examples. SAMSUNG-1003, [159].

As previously discussed (*see* [1.1], *supra*), in the combination, Kobylkin describes that the payment card “can be ***a substantially blank card***,” and “***can lack any information*** ... thereon.” *Id.*, [0017]. A POSITA would have understood that an account number encoded in an NFC or RFID code, as in Kobylkin, is not “visible.” SAMSUNG-1005, [0012], FIG. 5. Likewise, in embodiments where the account number is encoded as a QR code, the account number is not visible since it is masked by the QR coding and not easily discernible by a human. Thus,

Kobylkin teaches that the payment card information is not visible on the payment card. SAMSUNG-1003, [160].

Second alternative mapping

In the combination, the mobile device of Smith (*i.e.*, the computing device) is further operable to **receive**, **store**, and **transmit** the “mobile cloud account number” (MCA) (*i.e.*, card payment information) of a cardlet on the mobile device. SAMSUNG-1006, [0058]-[0059] (“Data that may be included in the mobile cloud account data may include the MCA and additional information discussed in more detail below. In step 434, the service provider 110 may transmit the post issuance script and related data to the mobile device 102, which may ***receive*** the script and data in step 436.”), [0051] (“mobile device 102 may be ready to ***receive*** MCAs for use in conducting contactless payment transactions”), [0061] (“***transmit*** the MCA and related payment credentials from the mobile cardlet in the secure ***storage*** to the contactless terminal 104 via near field communication”), [0067] (“mobile cloud account data ***stored*** in the secure element 210”), [0075] (“The MCA may be included in a mobile cloud account 704 provisioned to the wallet 202 of the mobile device 102. The wallet 202 may ***store*** the mobile cloud account 704 and related data (e.g., MCA, post issuance scripts, etc.)”), [0067]-[0068] (“payment credentials” including “MCA” transmitted from “mobile device 210” to a “contactless terminal 104”), FIGS. 4A, 6. SAMSUNG-1003, [161].

As previously discussed (Sections III.A.4-5, *supra*), in the combination based on Kobylkin, Smith's payment cards can be substantially blank and therefore would not have visible payment card information. SAMSUNG-1003, [162]. Moreover, the MCA would not be visible on any physical payment card device in the combination since the MCA is a number used only for transactions with mobile cloud accounts, as taught in Smith. SAMSUNG-1004, [0031], [0034]. The MCA is thus not printed or disposed on a payment card device, and certainly would not be printed, disposed, or otherwise made visible on a blank, disposable payment card of the type described in Kobylkin. *Supra*, [1.1]; SAMSUNG-1003, [162].

Limitation [1.9]

Smith describes that “the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102” to initiate “the transmission of *payment credentials* via near field communication from the mobile device 102 to the contactless terminal 104.” SAMSUNG-1004, [0067]. Smith teaches that the “payment credentials may include a *payment cryptogram*” (*i.e.*, a limited-use card payment information). *Id.* The payment cryptogram can be, for example, “an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210.” *Id.*, [0067], [0096], [0103]; SAMSUNG-1003, [164].

Also in the combination, Gomez describes that its payment card device

“generates an authentication cryptogram for each attempted transaction[.]”

SAMSUNG-1017, 5:25-28. Per Gomez, the cryptogram is generated ***“only after the cardholder successfully presents a credential***, such as a fingerprint or PIN number, into the payment card,” thereby indicating that the cryptogram (*i.e.*, the limited-use card payment information) is generated only for use by an authenticated user. *Id.*; SAMSUNG-1003, [165]; *see also* SAMSUNG-1004, [0068].

Limitation [1.10]

In the combination, Smith describes that “the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102” to initiate “the ***transmission of payment credentials via near field communication*** from the mobile device 102 to the contactless terminal 104.” SAMSUNG-1004, [0067]; *see also* [0061]. Smith teaches that the “payment credentials may include [the] ***payment cryptogram***” (*i.e.*, the limited-use card payment information). *Id.*, [0067], [0096], [0103]; SAMSUNG-1003, [167].

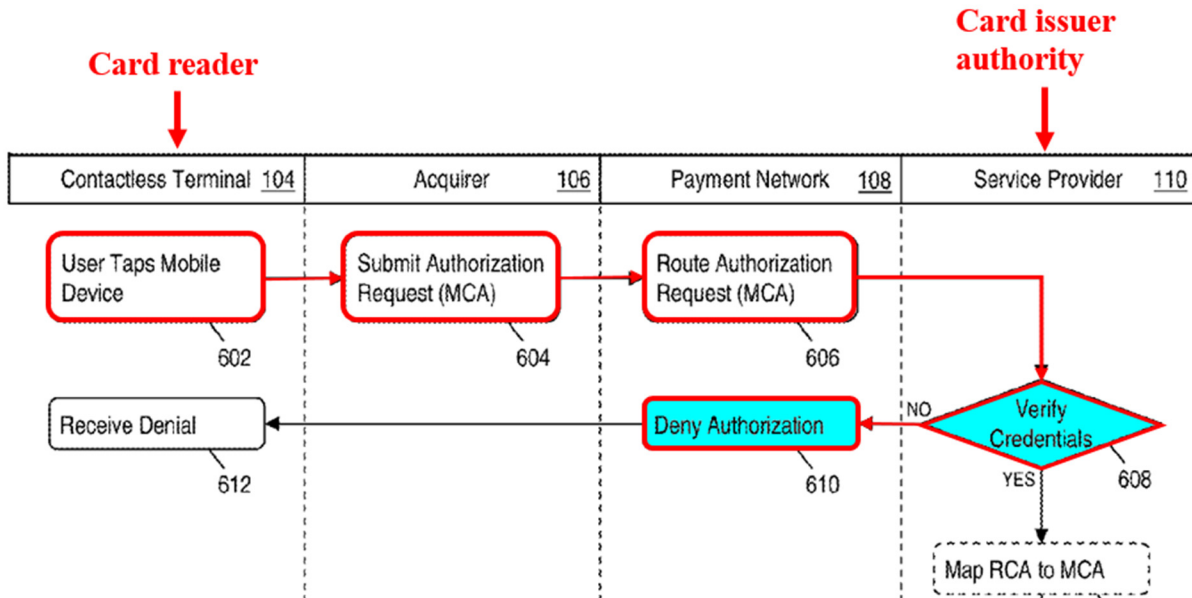
Limitation [1.11]

As previously discussed (*see* [1.10], *supra*), in the combination, Smith describes that the mobile device 102 transmits payment credentials to the contactless terminal 104 via near field communication to initiate a payment transaction. Smith describes that “[t]he contactless terminal 104 may forward the

payment credentials, including the MCA and payment cryptogram, to the acquirer 106, who may then submit an authorization request including the MCA and payment credentials to the payment network 108.” SAMSUNG-1004, [0067]; SAMSUNG-1003, [169].

Per Smith, “[t]he *service provider 110*” (*i.e.*, a card issuer authority) “may receive the MCA and additional payment credentials” from the payment network 108 “and may *verify (e.g., validate) the MCA and/or payment cryptogram* or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art.” *Id.*, [0070]. “*If the verification of the credentials fails*, then ... *the service provider 110 ... den[ies]*” the transaction. *Id.* A POSITA would have understood or found obvious that verification of payment credentials for an attempted transaction would fail if the attempted transaction was made outside of its limitations of use, such as if the payment cryptogram was expired, has previously been used, or did not validly correspond to the MCA contained in the payment credentials. SAMSUNG-1003, [170]. For example, in the combination, Gomez describes that “[a]ttempting to *re-use a previously generated authentication cryptogram* will” result in “a purchase transaction authorization *denial*.” SAMSUNG-1017, 5:39-41; SAMSUNG-1003, [170]. A transaction trying to reuse a previously used cryptogram would thus fail because it would be outside of its limitations of use. *Id.*

FIG. 6 from Smith shows the service provider 110 receiving and validating the payment credentials, including the payment cryptogram (step 608), and denying the transaction if the validation fails (step 610). *Id.*, [0070]; SAMSUNG-1003, [171]:



SAMSUNG-1004, Detail of FIG. 6 (annotated)

To the extent Patent Owner argues that the “issuer 112” in Smith must be the claimed card issuer authority rather than the “service provider 110,” Smith describes an embodiment where the issuer 112, rather than the service provider 110, validates the payment credentials and maps the MCA to RCA. *See* SAMSUNG-1004, [0072] (“In embodiments where the service provider 110 does not generate and map an MCA, the authorization response routed to the issuer 112 may include the MCA, and step 620 may further include identifying the RCA

corresponding to the MCA.”); SAMSUNG-1003, [172]. Smith also explains that “the service provider 110 ... may be operated by or on behalf of the issuer 112.” SAMSUNG-1004, [0037].

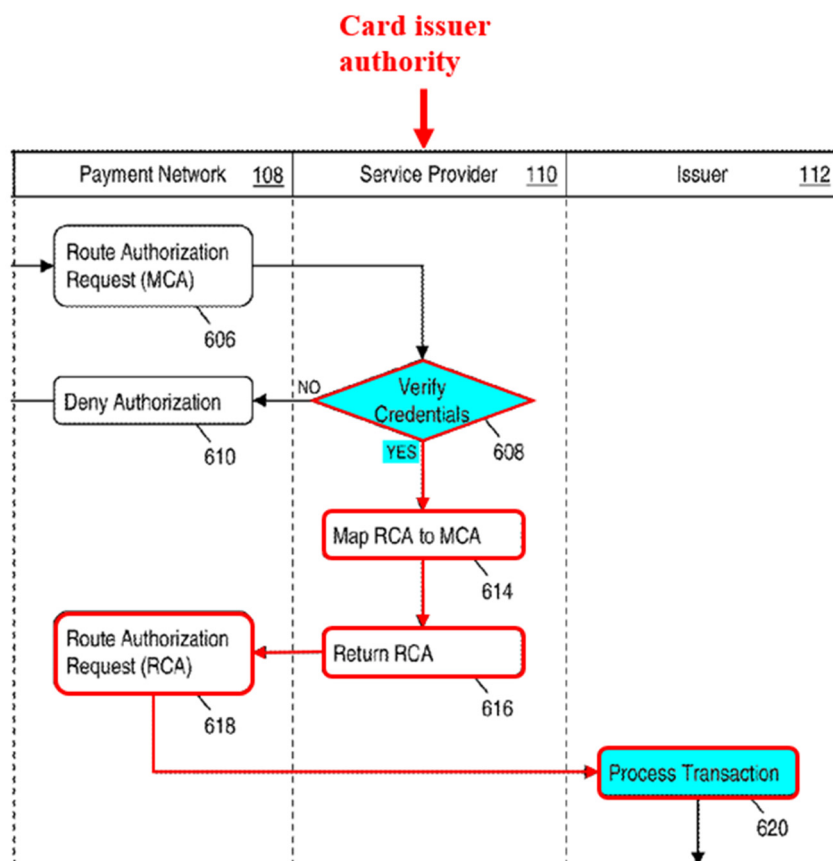
Limitation [1.12]

In the combination, Smith describes that “the mobile device 102 may also transmit additional credentials to the contactless terminal” such as “*a mobile personal identification number (PIN)*, which may be a number *input by the user* 302 into the mobile device 102 prior or subsequent to indication of an MCA for use in the payment transaction.” SAMSUNG-1004, [0068]. As described above (*see* [1.11], *supra*), Smith describes that the “service provider 110” (*i.e.*, the card issuer authority) “validates” the payment credentials, which include the “mobile personal identification number (PIN).” SAMSUNG-1004, [0068], [0070], FIG. 6 (step 608: “Verify Credentials”); SAMSUNG-1003, [174]. Moreover, as previously discussed, in the combination, the mobile device of Smith collects and validates a user PIN based on the teachings of Gomez. *See* Sections III.A.4-5, *supra*. A POSITA would have understood or at least found it obvious that a valid mobile PIN entered by the user indicates that the card payment information was received from an authenticated user’s computing device, because such functionality was well-known and in widespread use as of the Critical Date. SAMSUNG-1003, [174]; *see, e.g.*, SAMSUNG-1017, 5:25-28; SAMSUNG-1008,

[0019]-[0020]; SAMSUNG-1009, [0009].

Limitation [1.13]

As previously discussed (*see* [1.11], *supra*), in the combination, Smith describes that “[~~t~~]*he service provider 110*” (*i.e.*, the card issuer authority) “*validat[es] the MCA and/or payment cryptogram* or other credentials[.]” SAMSUNG-1004, [0070]. If the service provider 110 successfully validates the credentials, the service provider 110 permits the transaction to complete by forwarding the transaction details (with the MCA replaced by the mapped RCA) to the issuer 112, which “may approve and process the financial transaction using methods apparent to persons having skill in the relevant art.” SAMSUNG-1003, [176]; *see, e.g., id.*, [0071]-[0072]. The following annotated FIG. 6 from Smith shows this process:



SAMSUNG-1004, Detail of FIG. 6 (annotated)

(b) Claim 2

Limitation [2.0]

As previously discussed (*see* [1.5], *supra*), in the combination, Smith describes that the mobile device includes a “payment UI” that the user interacts with via a “touch screen” (*i.e.*, the touch-screen user interface). Smith further teaches that “*a mobile personal identification number (PIN)* ... may be a number *input by the user* 302 into the mobile device 102 prior or subsequent to indication of an MCA for use in the payment transaction.” SAMSUNG-1004, [0068]. A

POSITA would have understood or at least found it obvious that the user would “input” the mobile PIN into the mobile device via the payment UI (*i.e.*, the touch-screen user interface). SAMSUNG-1003, [180]; *see, e.g.*, SAMSUNG-1004, [0042], [0068], [0102]. In addition, a POSITA would have understood or at least found it obvious that the mobile PIN controls the user’s access to the payment transaction functionality of Smith’s mobile device (*i.e.*, the entered PIN must be authenticated in order to complete a payment transaction). SAMSUNG-1003, [180]; *see, e.g.*, SAMSUNG-1008, [0019]-[0020]; SAMSUNG-1009, [0009].

(c) Claim 7

Limitation [7.0]

See [1.8], [1.10], *supra*; SAMSUNG-1003, [183]-[186].

(d) Claim 8

Limitation [8.0]

See [1.8], [1.10], *supra*; SAMSUNG-1003, [187]-[189].

(e) Claim 9

Limitation [9.0]

See [1.8], [1.10], *supra* (the contactless terminal 104 is a “device”); SAMSUNG-1003, [190]-[192].

(f) Claim 10

Limitation [10.0]

In the combination, Smith describes that the payment UI (*i.e.*, the touch screen user interface) of the mobile device is operable to display (*i.e.*, transmit) payment information visually. SAMSUNG-1004, [0042], [0046], [0055], FIG. 2. Smith describes that “the payment UI 204 may ***display the mobile cloud account for the MCA*** to the user 302 ***in the form of an image of a payment card***” (*i.e.*, graphically). *Id.*, [0083]. Smith further describes that the “first twelve digits of the MCA obscured (e.g., replaced by asterisks) and ***the last four digits displayed***” (*i.e.*, alphanumerically) “such that the user 302 may readily recognize which MCA corresponds to which RCA based on the last four digits.” *Id.* “It will be apparent to persons having skill in the relevant art that ***other indicators may be used, such as a ... graphical representation of a physical payment card.***” *Id.* This graphical representation of the physical payment card in Smith is “iconography,” because it is a “representation” of the card, rather than the captured image described above. *Id.*; SAMSUNG-1003, [194].

(g) **Claim 12**

Limitation [12.0]

As previously discussed (*see* [1.12], *supra*), in the combination, Smith describes that “the mobile device 102 may also transmit additional credentials to the contactless terminal” such as “***a mobile personal identification number (PIN)***” (*i.e.*, a user passcode entry) “which may be a number ***input by the user*** 302 into the

mobile device 102 prior or subsequent to indication of an MCA for use in the payment transaction.” SAMSUNG-1004, [0068]. As described above (*see* [1.11], *supra*), Smith describes that the “service provider 110” (*i.e.*, a payment issuing authority) “validates” the payment credentials, which include the “mobile personal identification number (PIN),” and “den[ies] the transaction” if validation fails. SAMSUNG-1004, [0068], [0070], FIG. 6 (step 608: “Verify Credentials”); SAMSUNG-1003, [198]. A POSITA would have understood or at least found it obvious that entry of a PIN on a touchscreen of a mobile device like Smith’s constitutes a “security challenge” involving at least one of a user personal information question, a user passcode entry, a user touch-screen entry, a user touch-screen swipe, and/or a user gesture of a device. SAMSUNG-1003, [198]; *see, e.g.*, SAMSUNG-1004, [0068]; SAMSUNG-1010, [0187]-[0188].

Also in the combination, Gomez describes that the cryptogram is generated “only after the cardholder successfully presents a credential, ***such as a fingerprint or PIN number***, into the payment card.” SAMSUNG-1017, 5:25-28; SAMSUNG-1003, [199]; *see* [1.9], *supra*.

Limitation [12.1]

As described above (*see* [1.11], *supra*), Smith describes that the “service provider 110” (*i.e.*, a payment issuing authority) “validates” the payment credentials, which include the “mobile personal identification number (PIN),” and

“approv[es]” or “den[ies] the transaction” if validation fails. SAMSUNG-1004, [0068], [0070], [0072], FIG. 6 (step 608: “Verify Credentials”); SAMSUNG-1003, [201]. Also in the combination, Gomez describes that the cryptogram is generated “only after the cardholder successfully presents a credential, *such as a fingerprint or PIN number*, into the payment card.” SAMSUNG-1017, 5:25-28; SAMSUNG-1003, [201]; *see* [1.9], *supra*.

Limitation [12.2]

See [12.1], *supra*; SAMSUNG-1003, [203]-[205].

(h) Claim 13

Limitation [13.0]

As previously discussed (*see* [1.12], [12.0] *supra*), in the combination, Smith describes that “the mobile device 102 may also transmit additional credentials to the contactless terminal” such as “*a mobile personal identification number (PIN)*, which may be a number *input by the user* 302 into the mobile device 102 prior or subsequent to indication of an MCA for use in the payment transaction.” SAMSUNG-1004, [0068]. As described above (*see* [1.11], *supra*), Smith describes that the “service provider 110” (*i.e.*, a payment issuing authority) “validates” the payment credentials, which include the “mobile personal identification number (PIN),” and “den[ies] the transaction” if validation fails. SAMSUNG-1004, [0068], [0070], FIG. 6 (step 608: “Verify Credentials”); SAMSUNG-1003, [207]. A POSITA would have understood or at least found it

obvious that entry of a PIN constitutes a “security challenge.” SAMSUNG-1003, [207]; *see, e.g.*, SAMSUNG-1004, [0068]; SAMSUNG-1010, [0187]-[0188].

(i) Claim 14

Limitation [14.0]

See [13.0], *supra* (Smith describes that the mobile PIN is “input by the user 302 into the mobile device 102”); *see also* [12.0]-[12.1], *supra*; SAMSUNG-1003, [210]-[213].

(j) Claim 15

Limitation [15.0]

See [1.0], *supra*.

Limitation [15.1]

See [1.1], *supra*. In the combination, both Smith and Kobylkin make clear that the payment card reader can be operated by a “merchant.” *See, e.g.*, SAMSUNG-1004, [0031], [0035], [0036]; SAMSUNG-1005, [0015], [0032], [0048]; SAMSUNG-1003, [215].

Limitation [15.2]

See [1.2], *supra*.

Limitation [15.3]

See [1.5], [1.6], *supra*.

Limitation [15.4]

See [1.5], *supra*.

Limitation [15.5]

See [1.4], *supra*.

Limitation [15.6]

As previously discussed, the mobile device of Smith includes a memory. *See* [1.3], *supra*. In Smith, “FIG. 2 illustrates ***data stored*** in the mobile device 102 ***for use in conducting contactless payment transactions.***” SAMSUNG-1004, [0041]. The stored data includes “mobile account credentials” (*i.e.*, payment information) such as “the MCA for each mobile cloud account and one or more security key certificates.” *Id.*; SAMSUNG-1003, [220].

Limitation [15.7]

See [1.9], *supra*.

Limitation [15.8]

As previously discussed (*see* [1.10], *supra*), in the combination, Smith describes that “the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102” to initiate “the transmission of ***payment credentials*** via near field communication from the mobile device 102 to the contactless terminal 104.” SAMSUNG-1004, [0067]. Smith teaches that the “payment credentials may include a ***payment cryptogram***” (*i.e.*, the limited-use card payment information). *Id.*, [0067], [0096], [0103]; SAMSUNG-1003, [223].

Also in the combination, Gomez describes that the cryptogram is generated “only after the cardholder successfully presents a credential, ***such as a fingerprint***

or PIN number, into the payment card.” SAMSUNG-1017, 5:25-28; SAMSUNG-1003, [224]; *see* [1.9], *supra*; SAMSUNG-1004, [0068].

Limitation [15.9]

See [1.10], *supra* (Smith teaches that the “payment cryptogram” (*i.e.*, the limited-use card payment information) is received from the mobile device by the contactless terminal operated by the merchant. SAMSUNG-1004, [0067], [0096], [0103], FIG. 6); SAMSUNG-1003, [226].

Limitation [15.10]

As previously discussed (*see* [1.11], *supra*), in the combination, Smith describes that “[*t*]*he service provider 110*” (*i.e.*, a card issuing authority) “may receive the MCA and additional payment credentials” from the payment network 108 “and may *verify (e.g., validate) ... payment cryptogram*” (*i.e.*, the limited-use payment information) “using cryptography methods and systems apparent to persons having skill in the relevant art.” SAMSUNG-1004, [0070]; SAMSUNG-1003, [228]. Smith describes that this validation occurs when the mobile device is used for payment transactions at a “contactless terminal” operated by a “merchant.” SAMSUNG-1004, [0035]; SAMSUNG-1003, [228].

Limitation [15.11]

See [1.11], *supra*.

Limitation [15.12]

See [1.12], *supra*.

(k) Claim 16

Limitation [16.0]

As previously discussed (*see* [1.9], *supra*), in the combination, Smith describes that its payment card device is configured to dynamically generate a limited-use payment information (the “payment cryptogram”). Also in the combination, Gomez further discloses how a cryptogram for a transaction can be displayed on a device. SAMSUNG-1017, 13:1-4 (“cryptogram may be displayed”), 14:3-7; SAMSUNG-1003, [234].

Limitation [16.1]

See [15.9], *supra*.

(l) Claim 18

Limitation [18.0]

In the combination, Smith describes how a service provider wirelessly provides “mobile cloud account data” to the mobile device over-the-air (OTA), and explains that “the service provider 110 ... may be operated by or on behalf of the issuer 112.” SAMSUNG-1006, [0037], [0044], FIGS. 3-4. A POSITA would thus understand the “mobile cloud account data” as described in Smith to provide “issuer-provided payment information” as recited in [18.0]. SAMSUNG-1003, [239]. Smith further discloses that the system “transmit[s] ... eligible RCAs to the mobile device 102, for display to the user 302,” and “the user 302 may request an MCA for a real card account.” SAMSUNG-1004, [0055]-[0056], FIGS. 4A-4B. A

POSITA would have understood or at least found it obvious that Smith's personal computing device is configured to download account data from multiple issuers. SAMSUNG-1003, [239]; *see, e.g.*, SAMSUNG-1004, [0055]-[0056], [0069] ("The processing of payment transactions across multiple payment networks will be apparent to persons having skill in the relevant art."), FIGS. 4A-4B.

In addition, in the combination, Kobylkin describes the mobile device wirelessly downloading the card number of a disposable payment card via an NFC channel when a user uses his or her device to activate or fund the disposable payment card. SAMSUNG-1005, [0031], [0050], [0070]-[0071]. Kobylkin's card number is issued by an issuer of the disposable payment card, and constitutes another example of "card issuer provided payment card information" in the combination. *Id.*, [0023] ("payment provider can **issue** a plurality of blank cards"); SAMSUNG-1003, [240].

Limitation [18.1]

In the combination, Smith describes that the payment UI (*i.e.*, the touch screen user interface) of the mobile device enables the user to "***select*** an MCA for use in funding a contactless payment transaction." SAMSUNG-1004, [0059]; SAMSUNG-1003, [242].

As another example, Smith discloses that the system "transmit[s] ... eligible RCAs to the mobile device 102, for display to the user 302," and then "the user

302 may request an MCA for a real card account.” SAMSUNG-1004, [0055]-[0056], FIGS. 4A-4B. A POSITA would have understood and it would have been obvious that the user’s selection of an RCA (*i.e.*, an issuer-provided payment method) would occur via the touch-screen display interface of the device, similar to the selection of an MCA as depicted in FIG. 7. SAMSUNG-1003, [243]; *see, e.g.*, SAMSUNG-1004, [0031], [0034].

Limitation [18.2]

In the combination, Smith describes that the payment card device having an RCA is operable for payment transactions, and in particular, the payment card method having an RCA that corresponds to a user-selected RCA would be operable for a transaction with the user-selected RCA. SAMSUNG-1004, [0031], [0034]; SAMSUNG-1003, [245].

Smith further describes that, “[o]nce the MCA is selected... the mobile device 102 may be ready for the contactless payment transaction (e.g., ready to transmit payment credentials to the contactless terminal 104 via near field communication),” as discussed at [1.10], *supra*. SAMSUNG-1004, [0059]; SAMSUNG-1003, [246].

B. GROUND 1B – Claim 3 is obvious over Smith in view of Kobylkin, Gomez, and Saarisalo

1. Overview of Saarisalo

Saarisalo describes an NFC-enabled mobile device operable to perform

“card emulation” by transferring payment card information over NFC.

SAMSUNG-1011, [0001], [0004]. The device includes a “user interface...to enable the user to select different settings of the NFC component,” including enabling the user “to disable and enable card emulation all together.” *Id.*, [0104]-[0105].

2. The combination of Smith, Kobylkin, Gomez, and Saarisalo

In the combination, the user interface of the mobile device of Smith is modified to enable the user “to select different settings of the NFC component,” including enabling the user “to disable and enable card emulation all together,” as described by Saarisalo. SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1011, [0104]-[0105]; SAMSUNG-1003, [249].

3. Reasons to combine Smith, Kobylkin, Gomez, and Saarisalo

A POSITA would have been motivated and found it obvious to modify the user interface of the mobile device of Smith to enable the user “to select different settings of the NFC component,” including enabling the user “to disable and enable card emulation all together,” as described by Saarisalo. SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1011, [0104]-[0105]; SAMSUNG-1003, [250]. A POSITA would have been motivated to provide the user with additional control over the NFC functions of the mobile device, thereby allowing the user to disable

the NFC functions in situations where those functions are unnecessary (*e.g.*, because no payment transactions are taking) and/or in situations where a security risk exists (*e.g.*, when walking through a crowd where a significant risk of wireless “skimming” is present). SAMSUNG-1003, [250]; *see, e.g.*, SAMSUNG-1006, [0002]-[0003]; SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1011, [0104]-[0105].

Further, a POSITA would have found it obvious to modify Smith’s mobile device based on Saarisalo’s teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [251]. Here, “when a patent ‘simply arranges old elements with each performing the same function it had been known to perform’ and yields no more than one would expect from such an arrangement, the combination is obvious.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Saarisalo’s teachings to augment Smith’s mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith’s system. SAMSUNG-1003, [251].

In fact, a POSITA would have been motivated to implement the well-known techniques of Saarisalo in Smith’s mobile device to achieve the predictable benefits described in Saarisalo and elsewhere. SAMSUNG-1003, [252]; *see, e.g.*, SAMSUNG-1006, [0002]-[0003]; SAMSUNG-1004, [0042], [0055], [0102];

SAMSUNG-1011, [0104]-[0105]. Indeed, a POSITA would have had a reasonable expectation of success incorporating Saarisalo's teachings into Smith, because Saarisalo describes its techniques implemented in a mobile device similar to that of Smith. *See* SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1011, [0001], [0104]-[0105]; SAMSUNG-1003, [252].

Accordingly, for at least these reasons, augmenting Smith's device based on the teachings of Saarisalo would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 3

Limitation [3.0]

In the combination, Saarisalo describes an NFC-enabled mobile device operable to perform "card emulation" by transferring payment card information over NFC. SAMSUNG-1011, [0001], [0004]. The device includes a "***user interface...to enable the user to select different settings of the NFC component,***" including enabling the user "***to disable and enable card emulation all together,***" thereby enabling and disabling NFC payment transactions by the device. *Id.*, [0104]-[0105]; SAMSUNG-1003, [255].

C. GROUND 1C – Claim 4 is obvious over Smith in view of Kobylkin, Gomez, Saarisalo, and Slonecker

1. Overview of Slonecker

Slonecker describes a “system and method whereby a holder of a financial account card, such as a credit card or debit card, is able to disable and re-enable use of the card by locking and unlocking the card repeatedly.” SAMSUNG-1013, Abstract. Slonecker describes “provid[ing] a user interface for a card owner 12 to present a request to lock 16 or unlock 18 a financial account card to the card processor 24, wherein the locking or unlocking operation is implemented.” *Id.*, [0022]. Slonecker further describes that “transactions are not authorized for locked cards.” *Id.*, [0033].

2. The combination of Smith, Kobylkin, Gomez, Saarisalo, and Slonecker

In the combination, the user interface of Smith’s mobile device is modified to enable the user to lock and unlock the accounts (*e.g.*, MCAs) stored on the mobile device, based on the teachings of Slonecker. SAMSUNG-1003, [258]; *see, e.g.*, SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1013, Abstract, [0022], [0033].

3. Reasons to combine Smith, Kobylkin, Gomez, Saarisalo, and Slonecker

A POSITA would have been motivated and found it obvious to modify the user interface of the mobile device of Smith to enable the user “to disable and re-

enable use of a card by locking and unlocking the card,” as described by Slonecker. SAMSUNG-1003, [259]; *see, e.g.*, SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1013, Abstract, [0022], [0033]. A POSITA would have been motivated to provide the user with additional control over accounts managed by the mobile device, specifically by allowing the user to lock individual accounts from the mobile device in response to noticing fraudulent activity. SAMSUNG-1003, [259]; *see, e.g.*, SAMSUNG-1006, [0002]-[0003]; SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1013, Abstract, [0022], [0033]. Such functionality would reduce the number of completed fraudulent transactions, thereby leading to monetary savings for the card issuer. *See id.*

Further, a POSITA would have found it obvious to modify Smith’s mobile device based on Slonecker’s teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [260]. Here, “when a patent ‘simply arranges old elements with each performing the same function it had been known to perform’ and yields no more than one would expect from such an arrangement, the combination is obvious.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Slonecker’s teachings to augment Smith’s mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith’s system. SAMSUNG-1003, [260].

In fact, a POSITA would have been motivated to implement the well-known techniques of Slonecker in Smith's mobile device to achieve the predictable benefits described in Slonecker and elsewhere. SAMSUNG-1003, [261]; *see, e.g.*, SAMSUNG-1006, [0002]-[0003]; SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1013, Abstract, [0022], [0033]. Indeed, a POSITA would have had a reasonable expectation of success incorporating Slonecker's teachings into Smith, because Slonecker describes its techniques implemented in a mobile device similar to that of Smith. *See* SAMSUNG-1004, [0042], [0055], [0102]; SAMSUNG-1013, Abstract, [0022], [0033]; SAMSUNG-1003, [261].

Accordingly, for at least these reasons, augmenting Smith's device based on the teachings of Slonecker would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 4

Limitation [4.0]

In the combination, Slonecker describes a "system and method whereby a holder of a financial account card, such as a credit card or debit card, is able to disable and re-enable use of the card by ***locking and unlocking the card*** repeatedly." SAMSUNG-1013, Abstract. Slonecker describes "provid[ing] a user interface for a card owner 12 to present a request to lock 16 or unlock 18 a

financial account card to the card processor 24, wherein the locking or unlocking operation is implemented.” *Id.*, [0022]. Slonecker further describes that “*transactions are not authorized for locked cards.*” *Id.*, [0033]. Per Slonecker, “the locked condition of the card is distributed such that, when locked, use of the card to perform any transactions (other than an unlock transaction 18) is prevented.” *Id.*; SAMSUNG-1003, [264].

Limitation [4.1]

In the combination, Slonecker describes that “transactions are not authorized for locked cards.” SAMSUNG-1013, [0033]. Per Slonecker, when a card is unlocked, “the restored operable or unlocked status of the card is distributed such that *the card may once again be used for other transactions by the card owner 12.*” *Id.*, [0040]; SAMSUNG-1003, [266].

D. GROUND 1D – Claims 5, 11, and 17 are obvious over Smith in view of Kobylkin, Gomez, and Mestre

1. Overview of Mestre

Mestre describes a “payment-enabled mobile device such as a ‘smartphone’” that “incorporates risk management features that are applicable to its use in contactless payment transactions,” such as features “govern[ing] when verification of the cardholder’s identity is required for consummation of the current transaction.” SAMSUNG-1010, Abstract. Mestre describes that the “payment-enabled mobile telephone 102 prompts the user to enter his/her PIN.” *Id.*, [0140].

“For example, the payment-enabled mobile telephone 102 may present a screen display like that shown in FIG. 11.” *Id.*

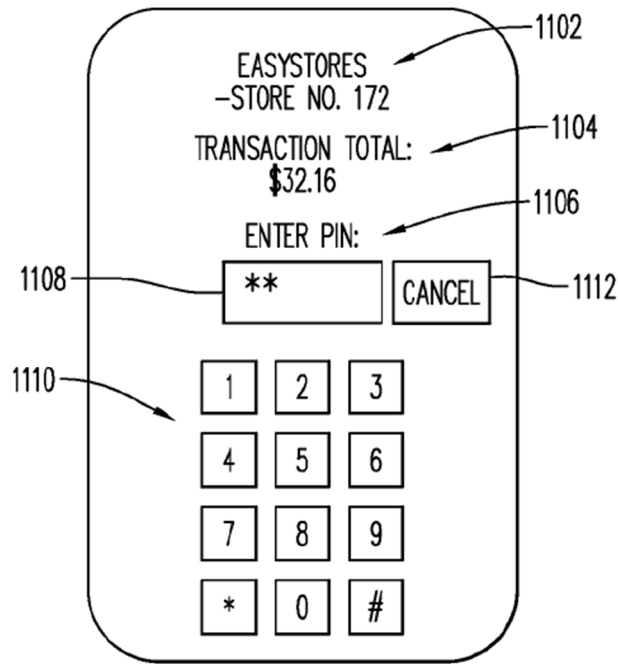


FIG. 11

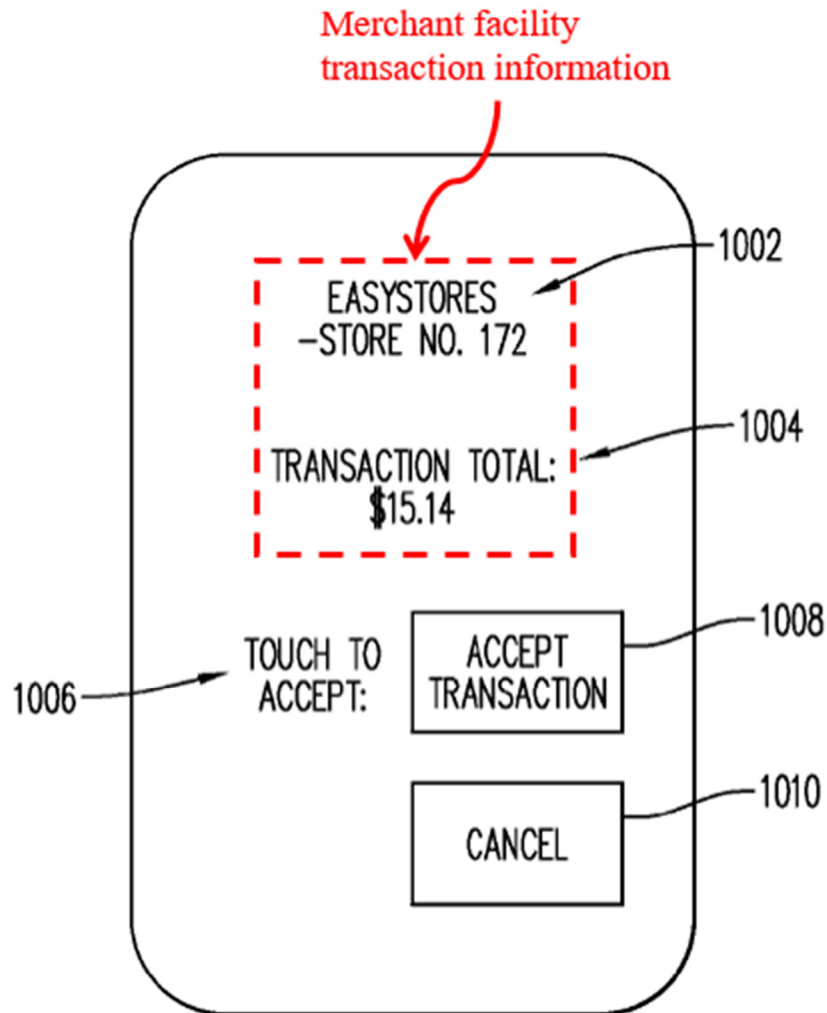
SAMSUNG-1010, FIG. 11

Mestre describes that “the payment application program determines whether the PIN, as entered by the user, is valid,” thereby authenticating the user. *Id.*, [0141].

Mestre further describes that “the payment-enabled mobile telephone 102 displays a prompt to the user to indicate that the user needs to accept the transaction” (*i.e.*, a merchant facility transaction). SAMSUNG-1010, [0091].

“FIG. 10 shows an example screen display that may be displayed to the user in this

case.” *Id.*:



SAMSUNG-1010, Detail of FIG. 10 (annotated)

2. The combination of Smith, Kobylkin, Gomez, and Mestre

In the combination, the mobile device of Smith displays a prompt to the user to indicate that the user needs to accept the transaction, based on the teachings of Mestre. SAMSUNG-1003, [269]; *see, e.g.*, SAMSUNG-1010, [0091], FIG. 10. Also in the combination, Smith’s mobile device is modified to operate in an

“offline-only” mode, like the device described in Mestre. SAMSUNG-1003, [269]; *see, e.g.*, SAMSUNG-1010, [0146]-[0147], [0150].

3. Reasons to combine Smith, Kobylkin, Gomez, and Mestre

A POSITA would have been motivated and found it obvious to display a prompt for the user to accept or deny a transaction and to operate in an “offline only mode,” based on the teachings of Mestre. SAMSUNG-1003, [269]. Smith describes one of its aims as “reducing the potential for fraud” in payment transactions performed by its system. SAMSUNG-1004, [0034]. Although Smith describes many mechanisms for securing the various sensitive information transferred between and stored by the components of its system, it focuses less on preventing fraud stemming from unauthorized use of the mobile device. *See, e.g., id.*, [0045] (describing a user merely selecting an MCA on the mobile device to initiate a payment transaction); SAMSUNG-1003, [269]. Implementing Mestre’s transaction approval in Smith’s mobile device would further Smith’s aim of “reducing the potential for fraud” by preventing the use of a stolen mobile device to initiate fraudulent transactions, such as by the mobile device verifying a user’s fingerprint prior to initiating a payment transaction and by allowing the user to deny fraudulent transactions he or she did not initiate, as taught by Mestre. SAMSUNG-1004, [0034], [0045]; SAMSUNG-1010, [0140]-[0141], FIG. 11; SAMSUNG-1003, [269].

Further, a POSITA would have found it obvious to modify Smith's mobile device based on Mestre's teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [270]. Here, "when a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Mestre's teachings to augment Smith's mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith's mobile device. SAMSUNG-1003, [270].

In fact, a POSITA would have been motivated to incorporate the well-known techniques of Mestre into Smith's mobile device to achieve the predictable benefits described in Mestre. SAMSUNG-1004, [0034], [0045]; SAMSUNG-1010, [0140]-[0141], FIG. 11; SAMSUNG-1003, [271].

Indeed, a POSITA would have had a reasonable expectation of success implementing Mestre's teachings in the context of Smith's mobile device, because Mestre implements its teachings in a device similar to Smith's. *See* SAMSUNG-1004, [0033]; SAMSUNG-1010, [0140]-[0141], FIG. 11; SAMSUNG-1003, [272].

Accordingly, for at least these reasons, augmenting Smith's mobile device based on the teachings of Mestre would have been routine and straightforward to a

POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 5

Limitation [5.0]

In the combination, Mestre describes an “offline-only” card device that “never goes online.” SAMSUNG-1010, [0150]; SAMSUNG-1003, [275]. A POSITA would have understood that such an “offline-only” card would lack a payment number information necessary for completing an online transaction. SAMSUNG-1003, [275]; *see, e.g.*, SAMSUNG-1010, [0146]-[0147], [0150]. A POSITA would have found it obvious to modify Smith’s mobile device to be “offline-only,” like the device described in Mestre, for the same reasons previously discussed at Section III.D.2-3.

Limitation [5.1]

As previously discussed (*see* [1.10], *supra*), in the combination, Smith describes that “the user 302 may ‘tap’ the contactless terminal 104 using the mobile device 102” to initiate “the transmission of payment credentials *via near field communication* from the mobile device 102 *to the contactless terminal 104.*” SAMSUNG-1004, [0067]; *see also* [0061]. Smith teaches that the “payment credentials may include [the] payment cryptogram.” *Id.*, [0067], [0096], [0103]; SAMSUNG-1003, [277]. Smith further describes that the mobile device may

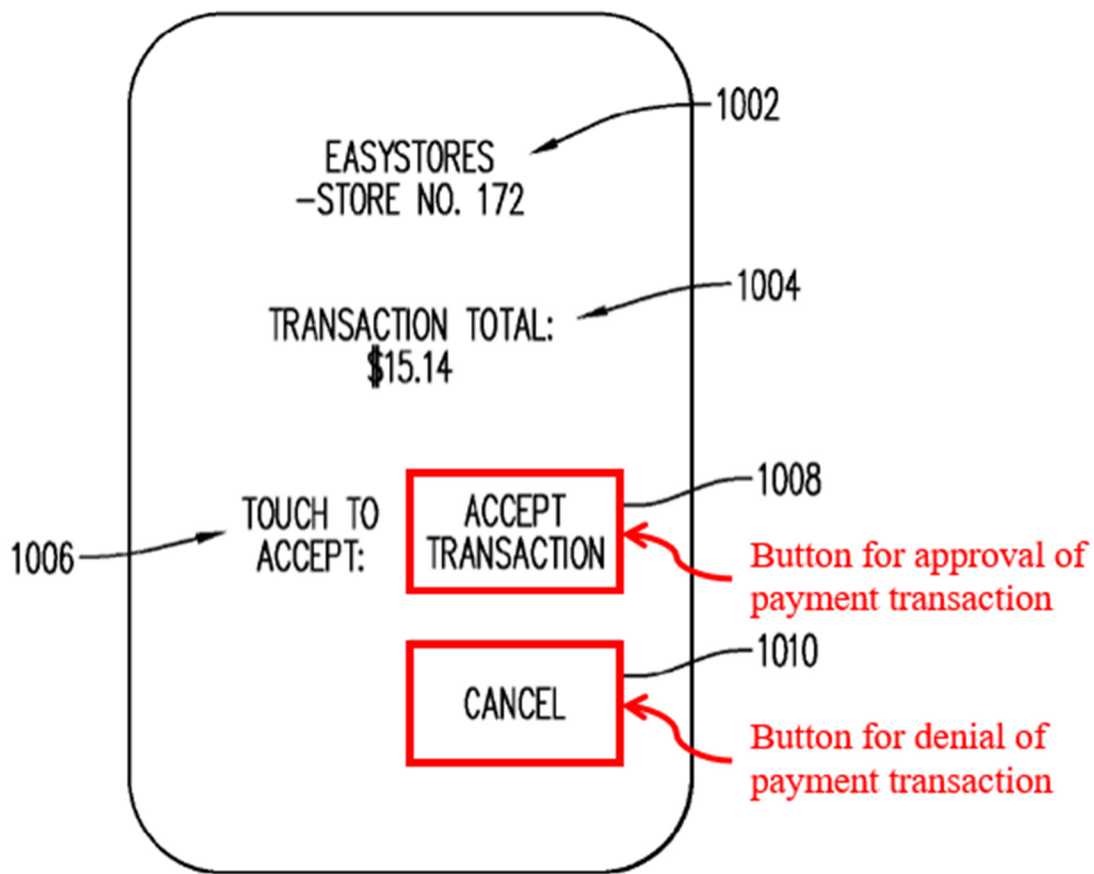
require a “mobile personal identification number (PIN)” and a separate “online PIN which may be input by the user 302 into the contactless terminal 104” (*i.e.*, which is limited to an in-store merchant card reader facility use only).

SAMSUNG-1004, [0068]; SAMSUNG-1003, [277].

(a) Claim 11

Limitation [11.0]

In the combination, Mestre describes that “the payment-enabled mobile telephone 102 *displays a prompt to the user* to indicate that *the user needs to accept the transaction*” (*i.e.*, a merchant facility transaction). SAMSUNG-1010, [0091]. Mestre describes that “the payment-enabled mobile telephone 102 displays the prompt to the user to *accept ... the transaction...by actuating (touching) the virtual ‘accept’ button* which appears at 1008.” SAMSUNG-1010, [0092]. “If the user wishes to *cancel the transaction, he/she may do so by touching the ‘cancel’ button 1010*, which is also provided as part of the screen display.” *Id.*; SAMSUNG-1003, [281]. This configuration is shown in FIG. 10 of Mestre:



SAMSUNG-1010, Detail of FIG. 10 (annotated)

Limitation [11.1]

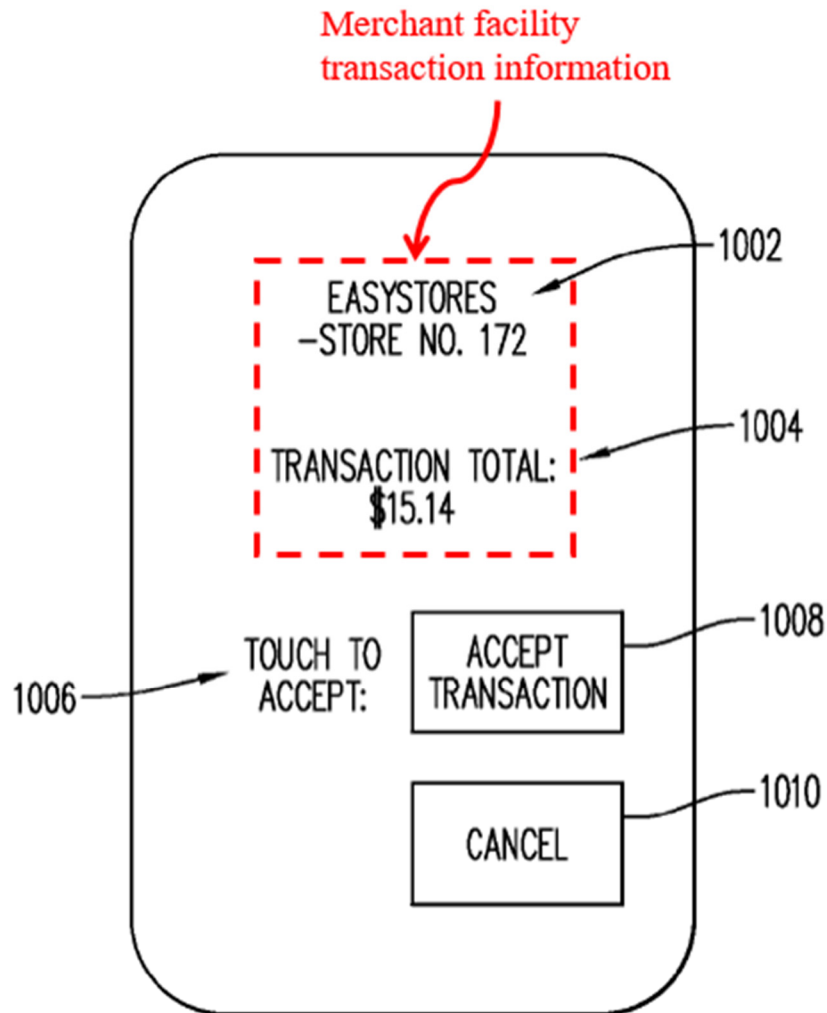
See Ground 1A [1.12], *supra*; SAMSUNG-1003, [283]-[284].

(b) Claim 17

Limitation [17.0]

In the combination, Mestre describes that “the payment-enabled mobile telephone 102 *displays a prompt to the user* to indicate that *the user needs to accept the transaction*” (*i.e.*, a merchant facility transaction). SAMSUNG-1010, [0091]. “FIG. 10 shows an example screen display that may be displayed to the

user in this case.” *Id.*; SAMSUNG-1003, [286]:



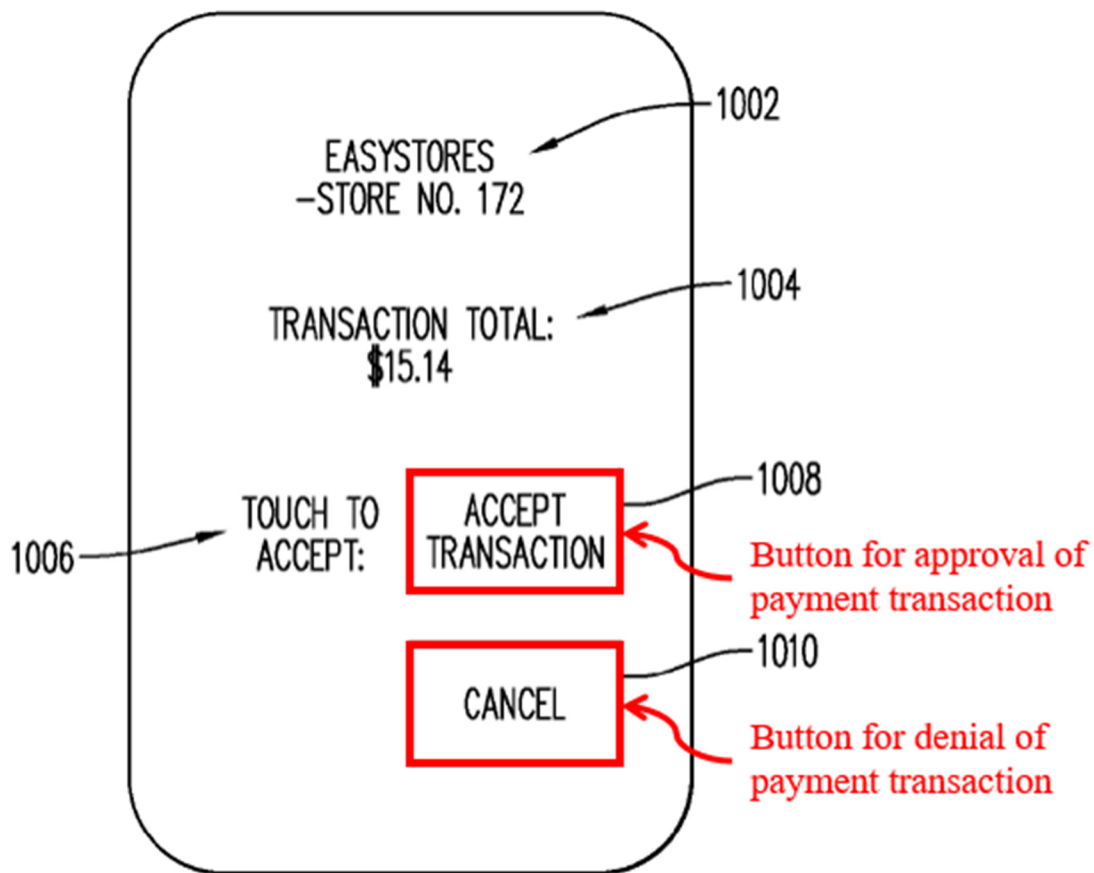
SAMSUNG-1010, Detail of FIG. 10 (annotated)

Limitation [17.1]

In the combination, Mestre describes that “the payment-enabled mobile telephone 102 displays the prompt to the user to *accept ... the transaction....by actuating (touching) the virtual ‘accept’ button* which appears at 1008.”

SAMSUNG-1010, [0092]. “If the user wishes to *cancel the transaction, he/she*

may do so by touching the ‘cancel’ button 1010, which is also provided as part of the screen display.” *Id.*; SAMSUNG-1003, [287]. This configuration is shown in FIG. 10 of Mestre:



SAMSUNG-1010, Detail of FIG. 10 (annotated)

Limitation [17.2]

See Ground 1A [1.12], Ground 1D [17.1], *supra*; SAMSUNG-1003, [289]-[290].

E. GROUND 1E – Claim 6 is obvious over Smith in view of Kobylkin, Gomez, and Sahota

1. Overview of Sahota

Sahota describes techniques “for dynamically generating a verification value for a transaction and for utilizing such value to verify the authenticity of the payment service application.” SAMSUNG-1006, Abstract. In particular, Sahota describes techniques for generating a dynamic card validation code on a “payment device,” referred to as a “dynamically generated Card Verification Value” or a “dCVV.” *Id.*, [0021], [0028]. Like the payment cryptogram or dynamic card validation code described in Smith, Sahota teaches that the dCVV “is generated on the payment device, embedded into the payment data, and transmitted to a point of sale terminal.” *Id.* Sahota further teaches that the dCVV “approach to authentication of the payment service ... significantly reduce[s] the opportunity for skimming since the verification value”—the dCVV—“is different for each transaction.” *See id.*, [0007], [0029].

Sahota teaches that the “payment device” stores an “application transaction counter (ATC)” in memory that is “incremented with each transaction.” *Id.*, [0028]. The ATC value is used (with other data) to generate a “dynamically generated Card Verification Value” or “dCVV,” which is “transmitted to a point of sale terminal” by the payment device when performing a payment transaction. *Id.*, [0021].

2. The combination of Smith, Kobylkin, Gomez, and Sahota

In the combination, the payment cryptogram or dynamic card validation

code of Smith is generated based on, or may be, the “dynamically generated Card Verification Value” or “dCVV” techniques described in Sahota. SAMSUNG-1003, [291]; *see, e.g.*, SAMSUNG-1006, [0007], [0021]-[0022], [0029]-[0031].

3. Reasons to combine Smith, Kobylkin, Gomez, and Sahota

A POSITA would have been motivated and found it obvious to generate the payment cryptogram of Smith based on the “dCVV” format described in Sahota. SAMSUNG-1003, [292]; *see, e.g.*, SAMSUNG-1006, [0007], [0021]-[0022], [0029]-[0031]; SAMSUNG-1004, [0067]. Smith describes that its payment cryptogram can be, for example, a “dynamic card validation code,” but does not include precise details on how such a code is generated. SAMSUNG-1004, [0067]. Sahota describes techniques for generating such a dynamic card validation code, referred to as a “*dynamically generated Card Verification Value*” or a “*dCVV*.” SAMSUNG-1006, [0021]. Due to the lack of specific implementation details for the “dynamic card validation code” in Smith, a POSITA would have been motivated to seek out such details, for example in Sahota. SAMSUNG-1003, [292]; *see, e.g.*, SAMSUNG-1006, [0007], [0021]-[0022], [0029]-[0031]; SAMSUNG-1004, [0067]. Sahota further describes that the “dCVV” is generated based partly on the “application transaction counter (ATC),” and thus Smith would also be modified to include this aspect of Sahota. *See* SAMSUNG-1006, [0028]-[0029].

Further, a POSITA would have found it obvious to modify Smith's mobile device based on Sahota's teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [293]. Here, "when a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Sahota's teachings to augment Smith's mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith's mobile device (to the extent those functions would be changed at all). SAMSUNG-1003, [293].

In fact, a POSITA would have been motivated to incorporate the well-known techniques of Sahota into Smith's mobile device to achieve the predictable benefits, described in both Smith and Sahota, of enabling the authenticity of a transaction to be validated based on the generated cryptogram. SAMSUNG-1004, [0011], [0034], [0045], [0063]; SAMSUNG-1006, [0007], [0021]-[0022], [0029]-[0031], [0038]; SAMSUNG-1003, [294].

Indeed, a POSITA would have had a reasonable expectation of success implementing Sahota's teachings in the context of Smith's mobile device, because Sahota implements its teachings in a device similar to Smith's. *See* SAMSUNG-

1004, [0033]; SAMSUNG-1006, [0007], [0021]-[0022], [0029]-[0031];
SAMSUNG-1003, [295].

Accordingly, for at least these reasons, augmenting Smith’s mobile device based on the teachings of Sahota would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 6

Limitation [6.0]²

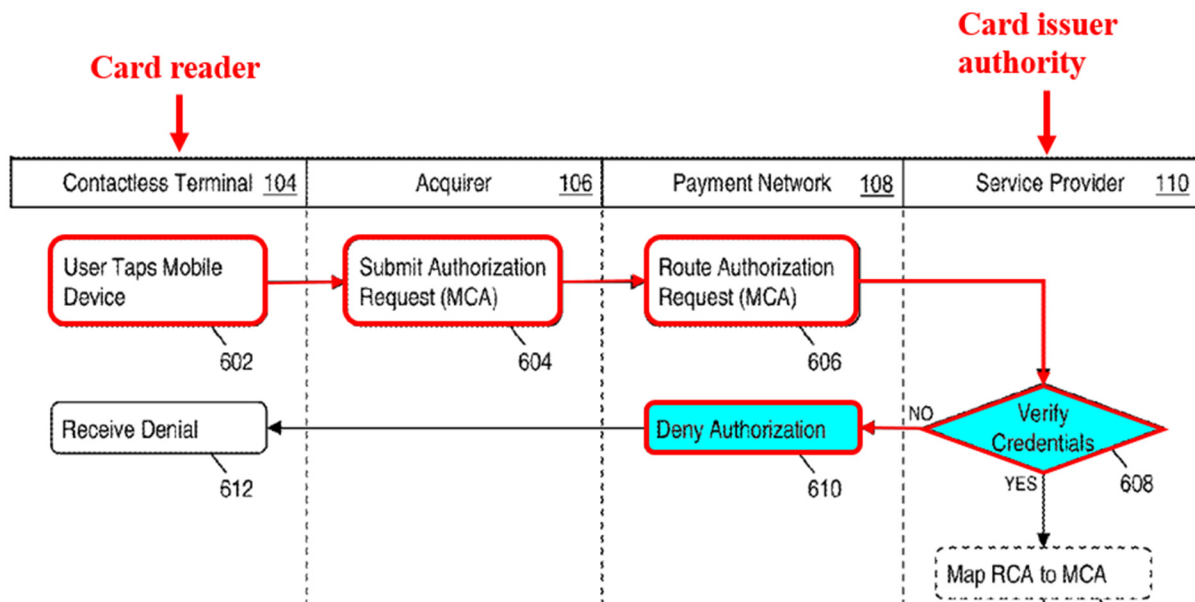
As previously discussed (*see* [1.10], *supra*), in the combination, Smith describes that the mobile device 102 transmits payment credentials to the contactless terminal 104 via near field communication to initiate a payment transaction. Smith describes that “[t]he contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram, to the acquirer 106, who may then submit an authorization request including the MCA and payment credentials to the payment network 108.” SAMSUNG-1004, [0067].

Per Smith, the “***service provider 110***” (*i.e.*, the card issuer authority, *see*

² For the purposes of this Petition only, it is assumed that “said transacted payment information”—which lacks antecedent basis—refers to the “card payment information” recited in [1.12].

[1.11], *supra*) “may **receive the MCA and additional payment credentials**” (*i.e.*, the transacted payment information) from the payment network 108.” *Id.*, [0070]; *see also* [0096] (the service provider “receive[s] transaction data related to a financial transaction”), FIG. 11; SAMSUNG-1003, [299].

FIG. 6 from Smith shows the service provider 110 receiving the payment credentials (step 608). SAMSUNG-1004, [0070]; SAMSUNG-1003, [300]:



SAMSUNG-1004, Detail of FIG. 6 (annotated)

Limitation [6.1]

As previously discussed (*see* [6.0], *supra*), in the combination, Smith describes that the service provider (*i.e.*, the card issuer authority) receives payment credentials (*i.e.*, card payment information) conveyed by the mobile device. Smith teaches that the “payment credentials may include [the] **payment cryptogram**” (*i.e.*,

the limited-use card payment information). SAMSUNG-1004, [0067], [0096], [0103]; SAMSUNG-1003, [302]; *see* [1.11], *supra*. Also in the combination, Gomez describes that the service provider “determines whether the authentication cryptogram is valid for the transaction...by *independently generating a ‘reference’ authentication cryptogram*” based on the same information used to generate the cryptogram on the payment device. SAMSUNG-1017, 6:23-38. “If the server-calculated reference authentication cryptogram matches the received authentication cryptogram generated by the” card device, the transaction is authenticated. *Id.*; SAMSUNG-1003, [302].

In addition, Smith describes that its payment cryptogram can be, for example, a “dynamic card validation code.” *Id.* Also in the combination, Sahota describes techniques for generating such a dynamic card validation code, referred to as a “*dynamically generated Card Verification Value*” or a “*dCVV*.” SAMSUNG-1006, [0021]. Like the payment cryptogram described in Smith, Sahota teaches that the dCVV “is generated on the payment device, embedded into the payment data, and transmitted to a point of sale terminal.” *Id.* Sahota further teaches that the dCVV “approach to authentication of the payment service ... significantly reduce[s] the opportunity for skimming since the verification value”—the dCVV—“*is different for each transaction.*” *See id.*, [0007], [0029].

Like Gomez, Sahota describes that “*the service provider computer will*

independently re-generate the dCVV” (*i.e.*, the payment cryptogram or limited-use payment information) “for the given transaction 645 *utilizing the same process*” used by the sending device (*i.e.*, Smith’s mobile device or a “point of sale terminal,” as described below). *Id.*

Sahota describes that “[e]ach time the payment service is initiated, *a dCVV is generated on the payment device for authentication purposes.*” *Id.*, [0029]; [0008] (the cryptogram “is dynamically generated on the payment device from data specific to the payment service”). Sahota describes that the dCVV is generated based on an “ATC” (*i.e.*, a sequence counter, *see* [1.7a], *supra*), an “account number for the payment service” (*i.e.*, a payment card account information), “the expiration date for the payment service and the service code” (*i.e.*, transaction information). *Id.*, [0029]; SAMSUNG-1003, [305]. A POSITA would have understood or at least found it obvious to generate the dCVV based, in addition, on a “merchant” and “facility information.” SAMSUNG-1003, [305]; *see, e.g.*, SAMSUNG-1006, [0021], [0023] (the dCVV can also include information from the point of sale terminal, which would include merchant and facility information). Further, Sahota describes that the dCVV is encrypted based on four encryption keys (120, 126, 130, 134 in FIG. 1), which are “secrets and an information limited to” the payment device. SAMSUNG-1006, [0029], FIG. 1; SAMSUNG-1003, [305].

Limitation [6.2]

In the combination, Sahota describes that “[i]f the service provider generated dCVV matches the dCVV received from the payment device 650, the service provider deems the payment application to be authentic 655.”

SAMSUNG-1006, [0038]; SAMSUNG-1003, [307]. A POSITA would have understood or at least found it obvious that the service provider would compare the generated dCVV to the received dCVV to determine whether the values match. *Id.*

Limitation [6.3]

In the combination, Sahota describes that “[i]f the service provider generated dCVV does not match the dCVV received from the payment device, the transaction is potentially fraudulent and is terminated 665.” SAMSUNG-1006, [0038]; SAMSUNG-1003, [309].

Limitation [6.4]

In the combination, Sahota describes that “[i]f the service provider generated dCVV matches the dCVV received from the payment device 650, the service provider deems the payment application to be authentic 655.”

SAMSUNG-1006, [0038]; SAMSUNG-1003, [311].

F. GROUND 1F – Claim 19 is obvious over Smith in view of Kobylkin, Gomez, and Moosavi

1. Overview of Moosavi

Moosavi describes a “mobile wireless communications device” that includes

a “Near Field Communications (NFC) integrated circuit ... operable with the processor for allowing the mobile wireless communications device to operate with other NFC enabled devices and conduct various transactions such as mobile ticketing, mobile payment, smart poster, Bluetooth Pairing, electronic tickets, and numerous other mobile commerce applications.” SAMSUNG-1015, 4:27-32. Moosavi describes disposing an “NFC logo on the housing of” the device to indicate the device’s support for NFC communication. SAMSUNG-1003, [114]-[116]; *see, e.g.*, SAMSUNG-1015, [0018].

2. The combination of Smith, Kobylkin, Gomez, and Moosavi

In the combination, the device of Smith includes the NFC logo printed thereon to indicate that the device is capable of NFC payments, as taught by Moosavi and as was well-known in the art as of the Critical Date. SAMSUNG-1003, [314]; *see, e.g.*, SAMSUNG-1015, [0018] (“It is also possible to have a *NFC logo* on the housing of the device”); SAMSUNG-1016, [0025] (“A logo/marking 46 indicating a wireless payment capability such as the *NFC logo*, a registered trademark of NFC Forum, Inc., is printed on top of the bottom cover 42.”).

3. Reasons to combine Smith, Kobylkin, Gomez, and Moosavi

A POSITA would have been motivated and found it obvious to include the NFC logo on the NFC-enabled mobile device described in Smith based at least on

the teachings of Moosavi. SAMSUNG-1003, [315]; *see, e.g.*, SAMSUNG-1015, [0018]; SAMSUNG-1016, [0025]. A POSITA would have been motivated to include the NFC logo on the housing of Smith's device in order to "indicat[e] [the] wireless payment capability" of Smith's device to users of the device. SAMSUNG-1016, [0025]; SAMSUNG-1015, [0018]; SAMSUNG-1003, [315].

Further, a POSITA would have found it obvious to modify Smith's mobile device based on Moosavi's teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [316]. Here, "when a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Moosavi's teachings to augment Smith's mobile device would have led to predictable results without significantly altering or hindering the functions performed by Smith's mobile device (to the extent those functions would be changed at all). SAMSUNG-1003, [316].

In fact, a POSITA would have been motivated to incorporate the well-known techniques of Moosavi into Smith's mobile device to achieve the predictable benefits, described in Moosavi, of indicating the NFC capability of Smith's mobile device to a user. SAMSUNG-1016, [0025]; SAMSUNG-1015,

[0018]; SAMSUNG-1003, [317].

Indeed, a POSITA would have had a reasonable expectation of success implementing Moosavi's teachings in the context of Smith's mobile device, because Moosavi implements its teachings in a device similar to Smith's. *See* SAMSUNG-1004, [0033]; SAMSUNG-1015, Abstract, [0018], FIG. 2; SAMSUNG-1003, [318].

Accordingly, for at least these reasons, augmenting Smith's mobile device based on the teachings of Moosavi would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 19

Limitation [19.0]

In the combination, Kobylkin describes that a “company name and/or ***logo of the provider of the instant disposable payment card***” (*i.e.*, a payment issuing logo) “can be ***printed on the instant disposable payment card.***” SAMSUNG-1005, [0018]. Kobylkin further describes that “***the user's name***” (*i.e.*, a card-holder name) “can be put on the instant disposable payment card.” *Id.* Kobylkin further describes that the “***payment provider name or logo***” (*i.e.*, a card payment network logo) can be “printed or otherwise provided on the instant disposable payment card.” *Id.*, [0029]; SAMSUNG-1003, [321].

Also in the combination, Moosavi describes disposing an “*NFC logo* on the housing of” a payment device supporting NFC communication. SAMSUNG-1003, [322]; *see, e.g.*, SAMSUNG-1015, [0018] (“It is also possible to have a *NFC logo* on the housing of the device”); SAMSUNG-1016, [0025] (“A logo/marking 46 indicating a wireless payment capability such as the *NFC logo*, a registered trademark of NFC Forum, Inc., is printed on top of the bottom cover 42.”).

Limitation [19.1]

As previously discussed, in the combination, Kobylkin describes that the thin payment device bears no fixed payment numbers. *See* [1.1], [15.1], *supra*.

G. GROUND 1G – Claims 20-27 are obvious over Smith in view of Kobylkin, Gomez, and Mullen

1. Overview of Mullen

Mullen describes a payment system in which a “message may ... be communicated from the authorization server” (i.e., an issuer) “to the mobile device to either authorize or deny the purchase transaction.” SAMSUNG-1007, [0051]; *see also id.*, [0286]-[0288] (“payment receipt”).

2. The combination of Smith, Kobylkin, Gomez, and Mullen

In the combination, the payment system described in Smith in the prior combination is modified to communicate the decision to authorize or deny a particular transaction back to the mobile device based on the teachings of Mullen. *See* SAMSUNG-1004, [0060]-[0065], FIG. 5; SAMSUNG-1007, [0051];

SAMSUNG-1003, [326]. In some examples, the communicated decision is conveyed to the mobile device in an electronic payment receipt. SAMSUNG-1007, [0051]; *see also id.*, [0286]-[0288] (“payment receipt”).

3. Reasons to combine Smith, Kobylkin, Gomez, and Mullen

A POSITA would have been motivated and found it obvious to modify the payment system described in Smith in the prior combination to communicate the decision to authorize or deny a particular transaction back to the mobile device based on the teachings of Mullen. *See* SAMSUNG-1004, [0060]-[0065], FIG. 5; SAMSUNG-1007, [0051]; SAMSUNG-1003, [327]. A POSITA would have been motivated to perform this modification in order to provide the user with access to more information about the transactions they have performed using the payment system, which would allow the user to more easily identify fraudulent transactions. SAMSUNG-1003, [327]; *see, e.g.*, SAMSUNG-1010, [0008] (emphasizing the importance of fraud detection and risk management in a payment system).

Further, a POSITA would have found it obvious to modify the payment system based on Mullen’s teachings because doing so entails the use of known solutions to improve similar systems and methods in the same way. SAMSUNG-1003, [328]. Here, “when a patent ‘simply arranges old elements with each performing the same function it had been known to perform’ and yields no more than one would expect from such an arrangement, the combination is obvious.”

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 417 (2007). A POSITA would have recognized that applying Mullen's teachings to augment the payment system would have led to predictable results without significantly altering or hindering the functions performed by the payment system. SAMSUNG-1003, [328].

In fact, a POSITA would have been motivated to incorporate the well-known techniques of Mullen into the payment system of the prior combination to achieve the predictable benefits described in Mullen and elsewhere. SAMSUNG-1003, [329]; *see, e.g.*, SAMSUNG-1007, [0051]; SAMSUNG-1010, [0008]. Indeed, a POSITA would have had a reasonable expectation of success incorporating Mullen's teachings into the payment system, because Mullen implements its teachings in a similar payment system. *See* SAMSUNG-1007, Abstract; SAMSUNG-1003, [329].

Accordingly, for at least these reasons, augmenting the payment system of the prior combination based on the teachings of Mullen would have been routine and straightforward to a POSITA, and it would have been clear that such a combination would predictably work and provide the expected results. *Id.*

4. Analysis

(a) Claim 20

Limitation [20.0]

See [1.0], *supra*.

Limitation [20.1]

See [1.1], *supra*.

Limitation [20.2]

See [1.2], *supra*.

Limitation [20.3]

See [1.3], *supra*.

Limitation [20.4]

See [1.4], *supra*.

Limitation [20.5]

See [1.5], *supra*.

Limitation [20.6]

See [1.6], *supra*.

Limitation [20.7]

In the combination, Smith teaches that the processor of the mobile device stores in the memory a “***mobile cloud account number (MCA)***” (*i.e.*, a static device account number) “which may be associated with a real card account number (RCA).” SAMSUNG-1004, [0034]; [1.7b], *supra*. The memory in the combination is further operable to store a transaction sequence count and secrets limited to the computing device as described above with respect to [1.7a] and [1.7c], *supra*. SAMSUNG-1003, [338].

Limitation [20.8]

See [1.8], *supra*. Additionally, in the combination and according to the first

mapping described above with respect to [1.8], Smith's mobile device is further operable, when used to fund and/or activate a disposable payment card like that described in Kobylkin (and to make purchases with the card), to display the card account number (*i.e.*, issuer-provided payment information) obtained from the disposable card. SAMSUNG-1005, [0087] ("The mobile device 120 can display ... the instant disposable payment card 150"), [0088] ("the code can be scanned with the user's mobile device and can be entered, either automatically or manually, into a form of the website"), [0031] ("The activation can take place completely manually via typing in or reading out over the phone."), [0072], [0136] ("card can be stored in and/or displayed upon a user device"). A POSITA would have understood and it would have been obvious that the card number would be displayed to the user after the card is scanned to permit the user to read it out over the phone to the payment provider or to permit the user to manually enter the card number into a form. SAMSUNG-1003, [340].

Kobylkin explains that the "payment provider can *issue*" the disposable payment cards, and the account number encoded on the issued cards would therefore constitute "issuer-provided payment information," as recited in [20.8]. SAMSUNG-1005, [0023]; SAMSUNG-1003, [341]. Additionally, as discussed above with respect to [1.1] and [1.8], the card account number is encoded on the disposable payment card device in an NFC or RFID code as taught in Kobylkin,

and is therefore “associated” with the payment card device; however, the card is otherwise “blank” and the card account number is not depicted on the payment card device. SAMSUNG-1005, [0017], [0050]; SAMSUNG-1003, [341].

Limitation [20.9a]

See [1.9], *supra*.

Limitation [20.9b]

In the combination, Smith teaches that the “payment cryptogram” (*i.e.*, the limited-use payment information, *see* [1.9], *supra*) and the MCA (*i.e.*, the static device account number, *see* [1.7b], *supra*) are combined into “payment credentials” and transmitted to the point-of-sale terminal to conduct a transaction.

See SAMSUNG-1004, FIG. 6, [0067]; SAMSUNG-1003, [344].

Limitation [20.10]

See [1.10], *supra*.

Limitation [20.11]

In the combination, Mullen describes that a “mobile device may, for example, communicate security credentials received from a physical card via a contactless communication channel to a network entity (e.g., an authorization server).” SAMSUNG-1007, [0051]. “Accordingly, for example, the authorization server may analyze the received security credentials and may either confirm or deny that the security credentials are authentic.” *Id.* Mullen describes that a “message may, for example, ***be communicated from the authorization server***”

(i.e., an issuer) “*to the mobile device to either authorize or deny the purchase transaction.*” *Id.* Mullen further describes a mobile device that receives an “electronic receipt” from an issuer in response to conveying payment credentials in a successful transaction indicating that the transaction is valid. SAMSUNG-1007, [0287] (“A payment receipt may, for example, be provided to mobile wallet 2802 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile wallet 2802 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation”), [0288] (“A payment receipt may, for example, be provided to mobile wallet 2802 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile wallet 2802 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.”); *see also id.*, [0210]-[0216], [0286], [0038], [0339]; SAMSUNG-1003, [347].

As previously discussed, it would have been obvious to a POSITA for the issuer or service provider in Smith to communicate information indicating that the payment transaction is valid to the mobile device, based on the teachings of Mullen. SAMSUNG-1003, [348]; *see, e.g.*, SAMSUNG-1007, [0051].

(b) Claim 21

Limitation [21.0]

See [18.0], *supra*. Smith’s “mobile cloud account data” includes the MCA

(*i.e.*, the static device account number, *see* [1.7b], *supra*). *See* SAMSUNG-1004, [0058], [0077]; SAMSUNG-1003, [351]-[354].

(c) Claim 22

Limitation [22.0]

As previously discussed (*see* [1.7a], *supra*), in the combination, Gomez describes a “payment card” including a “processor” that stores a “sequence value (or sequential number)” (*i.e.*, a transaction sequence count) that is “increment[ed] for each attempted use” of the card. SAMSUNG-1017, 7:24-26, 8:37-41, 10:34-42, FIG. 7; *see also* 10:66-11:2; SAMSUNG-1003, [356]. Gomez further teaches that the sequence value is used (with other data) to generate the “cryptogram,” which is limited-use payment information as previously discussed. SAMSUNG-1017, 2:45-50 (describing “generating an authentication cryptogram based at least in part on a...temporal signal value”), 7:24-26 (describing that the “temporal signal value may reflect the sequence value (or sequential number) of the attempted use”); SAMSUNG-1003, [356].

Limitation [22.1]

In the combination, Gomez describes that its payment card device “generates an authentication cryptogram *for each attempted transaction*[.]” SAMSUNG-1017, 5:25-28. Gomez further describes that “[a]ttempting to re-use a previously generated authentication cryptogram will” result in “a purchase transaction authorization denial,” thereby indicating that the cryptogram (*i.e.*, the generated

limited-use payment information) is valid only for a single use. *Id.*, 5:39-41;
SAMSUNG-1003, [358].

(d) Claim 23

Limitation [23.0]

See [1.7c], *supra*. The master key identifier and mobile cardlet of Smith are provided by the payment processing authority, and thus are payment processing authority secrets. SAMSUNG-1003, [361]-[364]; *see, e.g.*, SAMSUNG-1004, [0043]-[0045], [0056], FIG. 4A; [1.7c], *supra*.

(e) Claim 24

Limitation [24.0]

In the combination, Smith describes that “payment cryptogram” (*i.e.*, the limited-use payment information, *see* [1.9], *supra*) is generated based on the “mobile cloud account data.” *See* SAMSUNG-1004, [0103]. Per Smith, the “mobile cloud account data” includes the MCA (*i.e.*, the static device account number, *see* [1.7b], *supra*). *See* SAMSUNG-1004, [0058], [0077]; SAMSUNG-1003, [366]. Thus, Smith teaches that the “payment cryptogram” (*i.e.*, the limited-use payment information) is generated based on the “MCA” (*i.e.*, the static device account number).

(f) Claim 25

Limitation [25.0]

See [18.0], *supra*. Smith’s “mobile cloud account data” includes the MCA

(i.e., the static device account number, *see* [1.7b], *supra*). *See* SAMSUNG-1004, [0058], [0077]; SAMSUNG-1003, [369]-[372].

(g) Claim 26

Limitation [26.0]

See [24.0], *supra*.

(h) Claim 27

Limitation [27.0]

See [25.0], *supra*.

IV. DISCRETIONARY CONSIDERATIONS

None of the relied upon references were cited during prosecution. The facts associated with this Petition strongly favor institution, even under the *Fintiv* framework, as clarified by interim guidelines dated June 22, 2022. SAMSUNG-1016, 2.

Factor 1 (Stay)—Neither party has requested a stay.

Factor 2 (Trial Date)— Patent Owner’s complaint was filed on May 11, 2022 in the Eastern District of Texas (E.D. Tex.). SAMSUNG-1100. Based on a median time from filing to trial in E.D. Tex. of 24.5 months, trial is projected to occur in May, 2024. SAMSUNG-1103, 35; *Apple Inc. et al. v. Arigna Tech. Ltd.*, IPR2022-00651, Paper 12 at 9-12 (PTAB Oct. 6, 2022). A final written decision (“FWD”) is anticipated in July, 2024. The Board should not deny institution due to the close proximity of the expected FWD date and the predicted trial date in

E.D. Tex. SAMSUNG-1101, 3. Additionally, with a gap of just about two months between these dates—and with the median time to trial statistics in E.D. Tex. indicating that “delays are possible” with respect to the trial date set forth in the Court’s original scheduling order (*see* SAMSUNG-1104), the “efficiency and system integrity concerns that animate the *Fintiv* analysis are not as strong all other things being equal.” *Google LLC v. Parus Holdings, Inc.*, IPR2020-00846, Paper 9 at 14 (PTAB Oct. 21, 2020); IPR2022-00651, Paper 12 at 9-12.

Factor 3 (Investment)—The bulk of investment in the Related Litigation by the parties and court has yet to occur. Significantly, no part of claim construction and no document production has yet occurred. SAMSUNG-1104. By the time of institution in this proceeding, the Related Litigation will be at a similar posture where “much of the district court’s investment relates to ancillary matters untethered to the validity issue itself.” *Sand Revolution*, IPR2019-01393, Paper 24 at 10-11.

Factor 4 (Overlap)—Should PGR be instituted based on this Petition, Petitioner stipulates that it will not pursue in the Related Litigation any invalidity grounds against the Challenged Claims of the ’286 patent that are the same as

those raised in this Petition.³ Thus, if PGR is instituted, there will be no overlap or concerns of duplicative efforts. *See Sand Revolution*, Paper 24 at 11-12. Factor 4 thus weighs against discretionary denial. *Id.*; *Coolit Systems, Inc. v. Asetek Danmark A/S*, IPR2021-01995, Paper 10 at 12-13 (PTAB Dec. 28, 2021).

Factor 6 (Merits and Other Circumstances)—The strength of the merits alone justifies institution in the public interest and outweighs any inefficiencies born of parallel litigation. *See Fintiv* at 15; SAMSUNG-1101, 1. Petitioner has been diligent in filing this Petition just over four months after service of Patent Owner’s preliminary infringement contentions and identification of asserted claims on September 8, 2022. SAMSUNG-1105. In fact, Patent Owner identified more than ***100 asserted claims*** across five patents against Petitioner in its September 8, 2022 disclosure. Petitioner has worked diligently to develop invalidity grounds against each of the more than 100 asserted claims (and non-asserted claims), and began filing IPR or PGR petitions on the asserted patents without delay as early as November 2022. *See* IPR2023-00210, IPR2023-00211, IPR2023-00196, IPR2023-00219, IPR2023-00314.

V. CONCLUSION AND FEES

³ Petitioner reserves all rights to pursue these invalidity grounds in the Related Litigation if PGR on this Petition is not instituted.

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Samsung”) are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '286 patent is the subject of a civil action, *CardWare Inc. v. Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.*, 2:22-cv-00141, E.D. Tex., filed May 11, 2022 (SAMSUNG-1100). Petitioner is also filing a PGR petition challenging claims 1-27 of the '286 Patent under §§ 101 and 112. Petitioner is not aware of any other disclaimers, reexamination certificates, PGR petitions, or IPR petitions addressing the '286 patent.

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070/ Fax: 877-769-7945 Email: PGR39843-0147PS1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Daniel D. Smith, Reg. No. 71,278 Nicholas Stephens, Reg. No. 74,320 Patrick J. Bisenius, Reg. No. 63,893 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioner consents to electronic service by email at PGR39843-0147PS1@fr.com (referencing No. 39843-0147PS1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, nstephens@fr.com, dsmith@fr.com and bisenius@fr.com).

Respectfully submitted,

Dated 1/20/2023

/Daniel D. Smith/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Daniel D. Smith, Reg. No. 71,278
Nicholas Stephens, Reg. No. 74,320
Patrick J. Bisenius, Reg. No. 63,893
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. PGR2023-00012)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for Post Grant Review totals 16,964 words, which is less than the 18,700 allowed under 37 CFR § 42.24.

Dated 1/20/2023

/Daniel D. Smith/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Daniel D. Smith, Reg. No. 71,278
Nicholas Stephens, Reg. No. 74,320
Patrick J. Bisenius, Reg. No. 63,893
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on January 20, 2023, a complete and entire copy of this Petition for Post Grant Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

David Wyatt
c/o Murabito, Hao & Barnes
111 North Market Street, Suite 700
San Jose, CA 95113

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667