

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: David Wyatt
U.S. Patent No.: 10,628,820 Attorney Docket No.: 39843-0144IP1
Issue Date: April 21, 2020
Appl. Serial No.: 16/025,829
Filing Date: July 2, 2018
Title: MULTI-FUNCTION ELECTRONIC PAYMENT DEVICE

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 *INTER PARTES* REVIEW OF U.S. PATENT NO.
10,628,820 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42**

TABLE OF CONTENTS

I.	REQUIREMENTS FOR IPR	1
A.	Grounds for Standing.....	1
B.	Challenge and Relief Requested.....	1
C.	Claim Construction	3
1.	Claim limitations directed to printed matter are not entitled to patentable weight (claims 1-2, 11-12, 15-16)	3
2.	Additional non-limiting claim features	4
D.	Level of Ordinary Skill in the Art.....	4
II.	THE '820 PATENT.....	5
A.	Brief Description.....	5
B.	Prosecution History Overview.....	6
III.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	6
A.	[GROUND 1A]: Claims 1, 2, 6, and 10 are obvious over Mullen-876 in view of Kobylkin	6
1.	Overview of Mullen-876.....	6
2.	Overview of Kobylkin.....	7
3.	The combination of Mullen-876 and Kobylkin	8
4.	Reasons to combine Mullen-876 and Kobylkin.....	8
5.	Analysis	9
B.	[GROUND 1B]: Claims 3-5 and 7-8 are obvious over Mullen-876, Kobylkin, and Patel.....	21
1.	Overview of Patel.....	21
2.	The combination of Mullen-876, Kobylkin, and Patel	22
3.	Reasons to combine Mullen-876, Kobylkin, and Patel.....	23
4.	Analysis	24
C.	[GROUND 1C]: Claim 9 is obvious over Mullen-876, Kobylkin, and Smith	33
1.	Overview of Smith	33
2.	The combination of Mullen-876, Kobylkin, and Smith.....	34
3.	Reasons to combine Mullen-876, Kobylkin, and Smith	34
4.	Analysis	36
D.	[GROUND 2A]: Claims 11, 12, 15, 16-18, and 20 are obvious over Smith, Kobylkin, and Gomez	37
1.	Overview of Gomez	37
2.	The combination of Smith, Kobylkin, and Gomez	38
3.	Reasons to combine Smith, Kobylkin, and Gomez	39
4.	Analysis	43

E.	[GROUND 2B]: Claims 13 and 19 are obvious over Smith, Kobylkin, Gomez, and Varadarajan.....	64
1.	Overview of Varadarajan	64
2.	The combination of Smith, Kobylkin, Gomez, and Varadarajan	65
3.	Reasons to combine Smith, Kobylkin, Gomez, and Varadarajan.....	65
4.	Analysis	67
F.	[GROUND 2C]: Claim 14 is obvious over Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876	69
1.	The combination of Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876	69
2.	Reasons to combine Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876	69
3.	Analysis	70
IV.	DISCRETIONARY CONSIDERATIONS	71
V.	CONCLUSION AND FEES	73
VI.	MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....	74
A.	Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	74
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	74
C.	Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....	74
D.	Service Information	75

EXHIBITS

SAMSUNG-1001	U.S. Patent No. 10,628,820 to Wyatt (“the ’820 patent”)
SAMSUNG-1002	Excerpts from the Prosecution History of the ’820 patent (“the Prosecution History”)
SAMSUNG-1003	Expert Declaration and Curriculum Vitae of Michael Shamos, Ph.D.
SAMSUNG-1004	U.S. Pub. No. 2008/0302876 (“Mullen-876”)
SAMSUNG-1005	U.S. Pub. No. 2013/0166441 (“Kobylkin”)
SAMSUNG-1006	U.S. Pub. No. 2013/0232083 (“Smith”)
SAMSUNG-1007	U.S. Patent No. 9,600,808 (“Gomez”)
SAMSUNG-1008	U.S. Pub. No. 2008/0275779 (“Lakshminarayanan”)
SAMSUNG-1009	U.S. Pub. No. 2011/0082772 (“Hirson”)
SAMSUNG-1010	U.S. Pub. No. 2011/0191177 (“Blackhurst”)
SAMSUNG-1011	U.S. Pub. No. 2009/0144161 (“Fisher”)
SAMSUNG-1012	U.S. Pub. No. 2015/0178724 (“Ngo”)
SAMSUNG-1013	U.S. Pub. No. 2005/0043997 (“Sahota”)
SAMSUNG-1014	U.S. Pub. No. 2012/0143754 (“Patel”)
SAMSUNG-1015	U.S. Pub. No. 2011/0184867 (“Varadarajan”)
SAMSUNG-1016	U.S. Provisional Application Serial No. 61/794,891 (“the ’891 Provisional”)
SAMSUNG-1017	PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS E-commerce Guidelines (January 2013)

SAMSUNG-1018	PCI Data Security Standard, Navigating PCI DSS: Understanding the Intent of the Requirements, Version 2.0 (October 2010)
SAMSUNG-1019	Kadambi et al., <i>Near-Field Communication-Based Secure Mobile Payment Service</i> , ACM 11 th International Conference on Electronic Commerce 2009
SAMSUNG-1020	Todd Wasserman, <i>New Credit Card has LCD Screen, Touch-Sensitive Buttons</i> (Nov. 9, 2012)
SAMSUNG-1021	PCI Data Security Standard (PCI DSS), Information Supplement: PCI DSS Tokenization Guidelines, Version 2.0 (August 2011)
SAMSUNG-1022	Tim Carmody, WIRED, <i>The Smartphone in Your Pocket is a Multifunction Buying Machine</i> (Feb. 22, 2012), <i>available at</i> https://www.wired.com/2012/02/smartphone-buying-machine/ (retrieved December 22, 2022)
SAMSUNG-1023—1099	[RESERVED]
SAMSUNG-1100	Complaint for Patent Infringement, <i>Cardware Inc. v. Samsung Electronics Co., Ltd. et al.</i> , 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 B to CardWare Inc.’s P.R. 3-1 Disclosure of Asserted Claims and Infringement Contentions, <i>Cardware Inc. v. Samsung Electronics Co., Ltd. et al.</i> , Case No. 2:22-cv-00141 (E.D. Tex. (Sept. 8, 2022)
SAMSUNG-1103	United States District Courts National Judicial Caseload Profile, <i>available at</i>

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

Element	Claim Language
[1.0]	A payment device comprising:
[1.1]	a thin shaped body having no fixed payment numbers disposed thereon;
[1.2]	a memory;
[1.3]	a cryptographic processor coupled to the memory; and
[1.4]	a reader interface, including at least one interface selected from a set comprising a magnetic-stripe, a smart card reader interface, a mag-stripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and
[1.5]	wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and
[1.6]	wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities.
[2.0]	The device of claim 1, wherein the body comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo, and
[2.1]	wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.
[3.0]	The device of claim 1, wherein the limited-use payment information is conveyed via the magnetic-stripe and is unique to the payment device and to the magnetic stripe, and

Element	Claim Language
[3.1]	wherein the limited-use payment information is limited to use by the payment device and is operable for conveying payment information to a magnetic-stripe payment card reader, and
[3.2]	wherein said limited-use payment information has a limited period of valid use, and
[3.3]	wherein said limited-use payment information is not valid when used other than through a magnetic stripe payment card reader.
[4.0]	The device of claim 1, wherein said limited-use payment information is provided by a card issuing authority for use by the payment device and
[4.1]	wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.
[5.0]	The device of claim 1, wherein a request for payment includes at least one of a set comprising: payment information, transaction information, merchant information, and payment card reader information, and
[5.1]	wherein a card-present transaction is one including the limited-use payment information, and valid payment card reader information, and wherein a card-not-present transaction is one including at least a portion of said limited-use card payment information, and not including valid payment card reader information; and,
[5.2]	wherein a processing authority is operable to approve as valid, a card-present payment transaction; and,
[5.3]	wherein said card processing authority is operable to reject, as not valid, a use of the limited-use card payment information in a card-not-present payment transaction; and
[5.4]	wherein a card issuing authority receiving said request for payment is operable to decline a transaction not involving a valid card-present

Element	Claim Language
	use of a limited-use card payment information portion used in place of card issuer supplied payment information.
[6.0]	The device of claim 1, wherein a card processing authority is operable to reject as invalid, a use of the limited-use payment information provided via the reader interface, in online payment transactions.
[7.0]	The device of claim 1, wherein a card issuer providing the limited-use payment information, for use by the payment device, limits valid approval of said limited-use payment information to performing a card-present payment transaction by the card device, and wherein said card issuer declines as invalid a use of said limited-use payment information in transactions other than wherein the payment device is present, and
[7.1]	wherein a card issuer limits said card payment information to use for a finite amount of time, and declines as invalid use when said amount of time has expired, and
[7.2]	wherein a card issuer limits use to payment for transactions with the user approving, and declines as invalid use when the card user is denying an approval, and
[7.3]	wherein a card issuer limits to use in place of card issuer information for payments by the payment device.
[8.0]	The device of claim 1, wherein the reader interface is operable to wirelessly receive cardholder transaction information and to identify a valid user through at least one user-validation action, selected from a set of comprising:
[8.1]	a device touch ID sensor identifying a touch of the valid user; a device touch sensor-array receiving a user entered valid passcode; a device key-pad receiving a use entered a valid passcode; a device user interface receiving a user entered a valid PIN or Key-Code; a device user interface receiving a user entered a valid password; a device user interface reading a user swipe or gesture; a user tapping a predetermined sequence on the device; a user motioning the device

Element	Claim Language
	in accordance with a sequence; a skin-contact sensing identifying a valid user; a device sensor array reading a touch of an identified user; a device biometric recognition of a valid user; and a biometric sensing of the device remaining continuously in the possession of a valid user,
[8.2]	wherein a display of the device is operable to display transaction information through a user interface, and wherein transaction information includes at least one of a set comprising: a transaction time; a transaction amount; transaction merchant information; a transaction location; a transaction facility; card information; a partial card number; graphical card images; and
[8.3]	wherein upon validating the user, the user-interface is operable to receive a valid user input, of at least one user action selected from a set comprising: a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
[9.0]	The device of claim 1, wherein a dynamically-generated one-time limited-use payment information portion is generated by said processor when coupled to a reader interface accessible to said processor, and
[9.1]	wherein the payment information conveyed to a payment card reader, at the time of transaction, includes at least one of a portion of: a static limited-use portion; and a dynamically-generated limited-use portion, and
[9.2]	wherein said static limited-use payment information is provided by a card issuing authority for use in place of a card issuer payment information.
[10.0]	The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and at least one of a set of information including: a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information; an account

Element	Claim Language
	information; a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information; an account information; an amount; a transaction information; and a cryptographic combination of at least two of the above set of information, and
[10.1]	wherein the processor increments the card device transaction sequence count on each transaction.
[11.0]	An online payment system, the system comprising:
[11.1]	a thin payment device comprising no fixed payment numbers visible thereon; and
[11.2]	a personal computing device, wherein the personal computing device comprises a processor;
[11.3]	a memory;
[11.4]	a wireless interface;
[11.5a]	a display
[11.5b]	[the display] operable to provide a visual user-interface operable for performing online transactions; and
[11.6]	a user-interface coupled to the processor, and
[11.7]	wherein the wireless interface is operable to wirelessly obtain card device payment account information, and
[11.8]	wherein the processor is operable to, generate limited-use payment information based on the card device payment account information and
[11.9]	wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at

Element	Claim Language
	least one interface of a set comprising said display; and the wireless interface, and
[11.10]	wherein the limited-use payment information is configured to be used in place of a card issuer payment information.
[12.0]	The system of claim 11, wherein the thin payment device bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo.
[13.0]	The system of claim 11 wherein the personal computing device is configured for presenting on the display a limited-use card security code number for use in payments in place of card issuer payment information, and
[13.1]	wherein the personal computing device is further configured to generate said limited-use card security code responsive to an input request from a valid user, via said user-interface, and
[13.2]	wherein said limited-use number is generated on the personal computing device from at least one information from a set comprising: a payment device user information; a payment device account number; a payment device sequence counter; a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys; a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above.
[14.0]	The system as described in claim 11 wherein the personal computing device is configured for presenting on the display, a limited-use card account number, and a limited-duration expiration date, for use in payments in place of a card issuer payment information, and
[14.1]	wherein said personal computing device is further configured to generate said limited-use card payment information responsive to an input request from a valid user, and

Element	Claim Language
[14.2]	wherein the personal computing device is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising: a touch ID sensor operable to identify the touch a valid user; a user entering of a valid passcode on a touch sensor-array; a user entering of a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface; a user entering of a valid password on the user-interface; a valid user swiping or gesturing on a touch sensor-array; a valid sequence of a user tapping of the device detectable by device accelerometer; a valid user sequence of user motioning of the device detectable by device motion sensor unit; a skin-contact sensing identifying a valid user on a device contact sensor; a touching of an identified user's skin on a device touch sensor array; a device biometric recognition of a valid user via a device biometric sensing; and a biometric sensing of the device remaining continuously in the proximity possession of a valid user via device skin-proximity sensor; and, wherein the personal computing device conveys the limited-use payment information through the user interface.
[15.0]	An online payment system comprising:
[15.1]	a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and
[15.2]	a computing device operable for completing an online payment transaction and comprising a display;
[15.3]	a user-interface;
[15.4]	a processor; and
[15.5]	a memory for storing a payment card information accessible to the processor,
[15.6]	wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and
[15.7]	wherein at least one of the set comprising the computing device; and the card-shaped payment device, is configured to dynamically

Element	Claim Language
	generate a limited-use payment information, upon the authorization of a valid computing device user, and
[15.8]	wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.
[16.0]	The system of claim 15 wherein the card device bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.
[17.0]	The system of claim 15 wherein the dynamically generated limited-use payment information is displayable on a display of the computing device.
[18.0]	The system of claim 15 wherein the limited-use payment information includes a static limited-use card account number, a limited-duration card expiration date, and a limited-use card security code and,
[18.1]	wherein the dynamically generated limited-use payment information is conveyed by the computing device to complete an online transaction.
[19.0]	The system of claim 15 wherein the computing device is operable to generate a limited-use card security code number, for use in place of a card issuers card security code by generating said limited-use number via cryptographically combining information from at least one of a set comprising: a user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set, and
[19.1]	wherein the computing device is operable to display the generated limited-use card security code on the display.
[20.0]	The system of claim 15 wherein the computing device is further operable to obtain a user payment approval through at least one user-

Element	Claim Language
	interface element of the computing device, from a set comprising: a display interface, a touch-screen interface, a touch ID button, input buttons, a touch key-pad, a key-pad, a key-board, an optical sensor array, a motion detection unit, an accelerometer, the swiping of a recognized user skin over a device sensor array, a biometric sensor, a wireless interface, an NFC interface, an RF interface, a device biometric sensing the device is continuously remaining in contact with a valid user; and
[20.1]	wherein the computing device is operable to display at least one of a set comprising the transaction information, the merchant information, the time, the location of the transaction, the payment bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device, and, a user input providing for at least one user action from a set comprising an approving of a transaction, a denying of a transaction, and an adjusting of a transaction, via the user-interface.

Samsung Electronics Co., Ltd. (“Petitioner” or “Samsung”) petitions for *Inter Partes* Review (“IPR”) of claims 1-20 (“the Challenged Claims”) of U.S. Patent No. 10,628,820 (“the ’820 patent”).

I. REQUIREMENTS FOR IPR

A. Grounds for Standing

Petitioner certifies that the ’820 patent is available for IPR. This petition is being filed within one year of service of a complaint against Samsung.

SAMSUNG-1100. Samsung is not barred or estopped from requesting review of the Challenged Claims on the below-identified grounds.

B. Challenge and Relief Requested

Samsung requests an IPR of the Challenged Claims on the grounds noted below. Dr. Shamos provides supporting testimony in his Declaration (SAMSUNG-1003).

Ground	Claim(s)	35 U.S.C. § 103 Basis
1A	1-2, 6, 10	Mullen-876 in view of Kobylkin
1B	3-5, 7-8	Mullen-876 in view of Kobylkin and Patel
1C	9	Mullen-876 in view of Kobylkin and Smith
2A	11-12, 15-18, 20	Smith in view of Kobylkin and Gomez
2B	13, 19	Smith in view of Kobylkin, Gomez, and Varadarajan
2C	14	Smith in view of Kobylkin, Gomez, Varadarajan, and Mullen-876

The '820 patent claims priority to a provisional application filed on March 15, 2013 ("Critical Date"). Petitioner has applied prior art that predates this date and has used the Critical Date as the date of invention for purposes of this IPR.¹ Each of the prior art references applied in the above-listed Grounds qualifies as prior art to the '820 patent as shown below:

Reference	Dates	AIA Prior Art Basis
Mullen-876	Dec. 11, 2008 (published)	35 U.S.C. § 102(a)(1)
Kobylkin	Dec. 21, 2012 (filed) Dec. 22, 2011 (priority)	35 U.S.C. § 102(a)(2)
Smith	March 1, 2013 (filed) March 1, 2012 (priority)	35 U.S.C. § 102(a)(2)
Gomez	Jun. 22, 2012 (filed)	35 U.S.C. § 102(a)(2)
Patel	Jun. 7, 2012 (published)	35 U.S.C. § 102(a)(1)
Varadarajan	Jul. 28, 2011 (published)	35 U.S.C. § 102(a)(1)

None of these references were considered during prosecution of the '820

¹ Petitioner does not concede that any of the Challenged Claims enjoy priority to the March 15, 2013, filing date of the provisional application. Indeed, multiple claims of the '820 patent recite features that are plainly not described in the provisional application. SAMSUNG-1003, ¶¶24-26. The analysis presented in this petition remains the same regardless of whether March 15, 2013 or March 17, 2014 is used as the date of invention.

patent.

C. 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, ¶¶73-76.

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 is not conceding that the Challenged Claims satisfy all statutory requirements including those under 35 U.S.C. § 112.

1. Claim limitations directed to printed matter are not entitled to patentable weight (claims 1-2, 11-12, 15-16)

The Challenged Claims include various limitations directed to printed matter that have no functional or structural relationship to the claimed substrate on which the information is disposed or printed. The Federal Circuit has repeatedly emphasized 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 claim limitations shown in the following table are directed to printed matter, and thus are entitled to no patentable weight. Nonetheless, as described in greater detail in Section III, and regardless of whether these limitations are ultimately deemed to have any patentable weight, they are nonetheless rendered obvious by the prior art combinations presented in this Petition.

Claim	Language
1	“having no fixed payment numbers disposed thereon”
2	“the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo” / “free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.”
11	“comprising no fixed payment numbers visible thereon”
12	“bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo”
15	“bears no fixed payment numbers on the card device”
16	“bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.”

2. Additional non-limiting claim features

The features recited in claim elements [4.0]-[4.1], [5.0]-[5.4], [6.0], and [7.0]-[7.3] are not limiting as they do not define further limitations of the recited payment device. These features are nonetheless obvious for the reasons described in detail below in Section III.

D. 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, ¶¶42-47. Additional education could substitute for professional experience, or vice versa. *Id.*

II. THE '820 PATENT

A. Brief Description

The '820 patent describes itself as “generally relate[d] to electronic or smart multi-function electronic devices and, more specifically, to more secure, smart multi-function electronic payment devices and transaction processing thereof.” SAMSUNG-1001, 1:27-31. A magnetic strip on the card can be “encoded with a limited-duration credit card number that is associated with [a] selected account” and that can be communicated to a merchant terminal in a payment transaction. *Id.*, 7:50-52.

However, as shown below and addressed by Dr. Shamos, the concepts of “limited-duration” and “limited-use” payment card numbers, and techniques to generate them on mobile devices on a per-transaction basis, were well-known in the art prior to the Critical Date. SAMSUNG-1003, ¶¶29-32. Indeed, as Dr. Shamos explains, the state of the art in relation to limited-duration and limited-use

payment card numbers was already well developed before the Critical Date, with the claimed techniques having been described extensively in industry standardization documents, patents, and various other literature before the alleged invention. *Id.*, ¶¶48-72.

B. Prosecution History Overview

Examination of the application that issued as the '820 patent was brief and involved no prior art rejections. *See generally* EX1002. There is no indication in the file history that the Examiner substantively considered any of the prior art references or combinations relied upon in this Petition, which compellingly demonstrate that the Challenged Claims are obvious and should not have been allowed. SAMSUNG-1003, ¶¶33-41.

III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. [GROUND 1A]: Claims 1, 2, 6, and 10 are obvious over Mullen-876 in view of Kobylkin

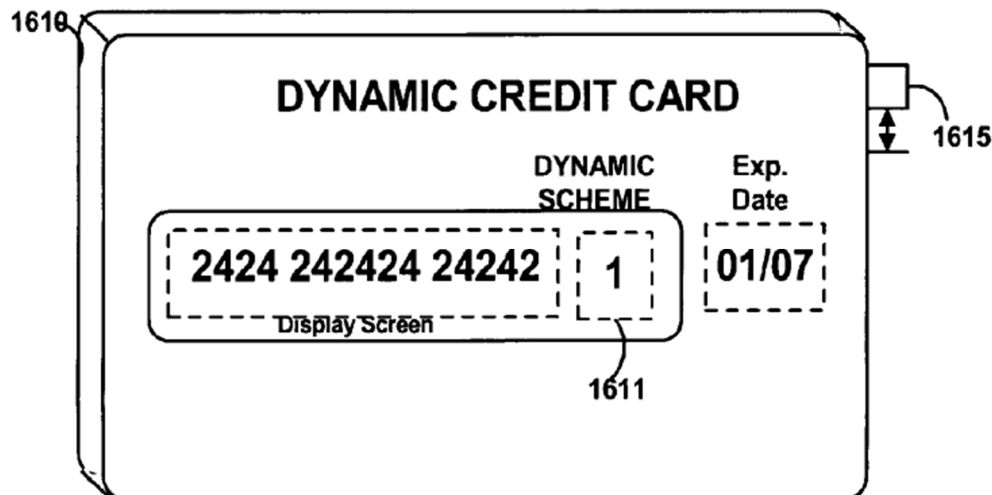
1. Overview of Mullen-876

Mullen-876 describes a “dynamic credit card” that is operable to encode “a secure credit card number (e.g., a secret/hidden credit card number)...based on a timing signal (e.g., an internal counter) to provide a dynamic credit card number.” SAMSUNG-1004, Abstract, [0049].

Mullen-876 describes that the “dynamic number may be displayed to a user via [the] display (e.g., so that online purchases can be made) or written onto a

magnetic stripe such that the number may be processed by traditional credit card merchants (e.g., swiped).” *Id.* Mullen-876 further describes that the dynamic credit card number may be “limited to only one use and, as such ... a dynamic number (e.g., a dynamic credit card number or verification code) may not repeat for the life of a dynamic credit card (e.g., 1 to 5 years).” *See* SAMSUNG-1004, [0121]; *see also* SAMSUNG-1003, ¶¶77-81.

FIG. 16 from Mullen-876 shows the dynamic credit card:



SAMSUNG-1004, Detail of FIG. 16

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]; SAMSUNG-1003, ¶¶82-85.

3. The combination of Mullen-876 and Kobylkin

In the combination, the dynamic credit card of Mullen-876 is implemented as a “substantially blank card,” 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, ¶¶103-105; *see, e.g.*, SAMSUNG-1004, Abstract, [0049], [0121], FIG. 16; SAMSUNG-1005, [0015]-[0018]. Further, in the combination, dynamic payment numbers can be presented to the user on an electronic display of the dynamic credit card, or the card may lack a display such that no payment numbers are presented to the user. SAMSUNG-1004, [0016], FIG. 16; SAMSUNG-1003, ¶105.

4. Reasons to combine Mullen-876 and Kobylkin

A POSITA would have been motivated and found it obvious to implement the dynamic credit card of Mullen-876 to include only selected, non-confidential information on its face according to the teachings of Kobylkin. SAMSUNG-1003, ¶¶106-108. A POSITA would have understood that the dynamic credit card of

Mullen-876 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, ¶¶106-108; *see, e.g.*, SAMSUNG-1004, [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].

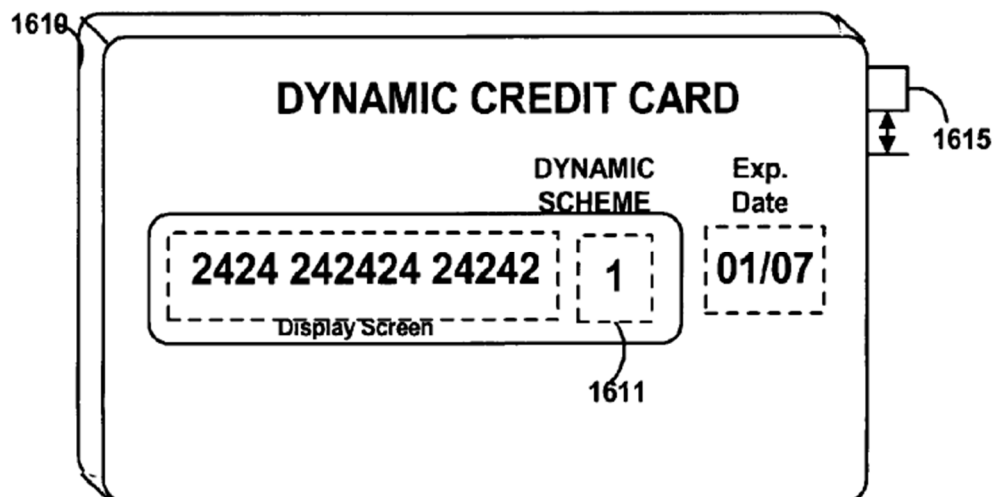
Further, a POSITA would have found it obvious to combine the teachings of Mullen-876 and Kobylkin because doing so entails the mere use of known solutions to improve similar systems and methods in the same way (e.g., similar payment cards). SAMSUNG-1003, ¶107. Here, “when a patent ‘simply arranges old 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 Kobylkin’s teachings to Mullen-876 would have led to predictable results without significantly altering or hindering the functions performed by Mullen-876 system. SAMSUNG-1003, ¶¶107-108.

5. Analysis

(a) Claim 1

Element [1.0]

To the extent the preamble is limiting, the combination of Mullen-876 and Kobylkin renders it obvious. SAMSUNG-1003, ¶¶109-110. For example, in the combination, Mullen-876 describes a “***dynamic credit card***” that is operable to encode “a secure credit card number (*e.g.*, a secret/hidden credit card number)...based on a timing signal (*e.g.*, an internal counter) to provide a dynamic credit card number.” SAMSUNG-1004, Abstract.² Per Mullen-876, the “dynamic credit card” is a computing device including “display circuitry,” a “display,” “memory,” and a “processor,” along with credit card features such as a “magnetic stripe[.]” *Id.*, [0076]; *see also* [0049]; SAMSUNG-1003, ¶110. FIG. 16 from Mullen-876 shows the dynamic credit card displaying a dynamic credit card number on an integrated display screen:



² All emphasis added unless otherwise indicated.

Mullen-876 further describes that “a user can *purchase items using [the] dynamic credit card* and a processing facility can authorize such purchases by recognizing that [the] dynamic number is valid (*e.g.*, valid for a particular period of time).” *Id.*, [0051]. Accordingly, Mullen-876 teaches that the “dynamic credit card” is a “payment device,” and thus the combination renders this limitation obvious.

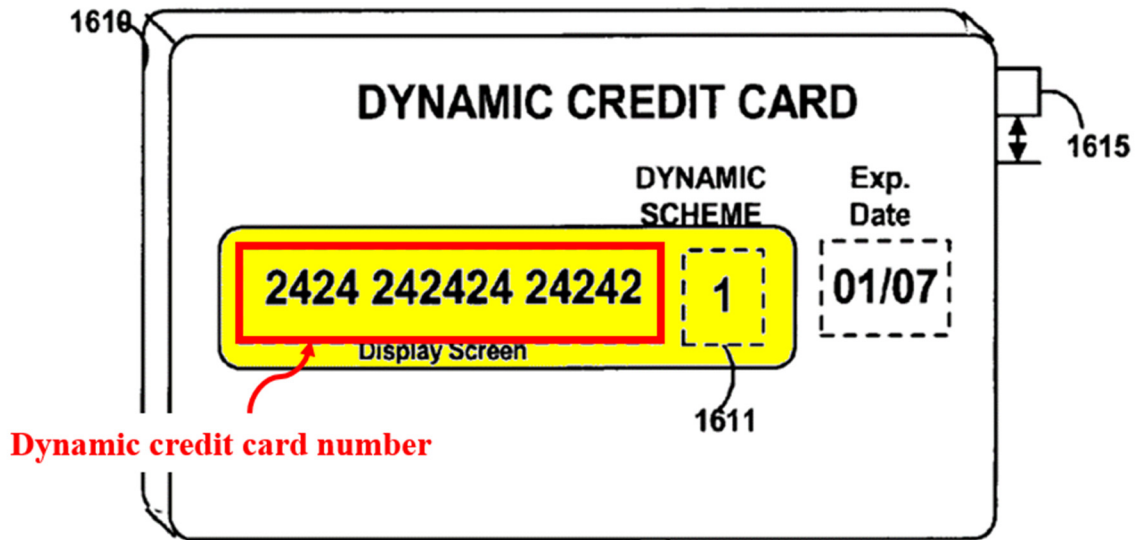
Element [1.1]

As previously discussed (*see* Section, I.C, *supra*), the limitation “having no fixed payment numbers disposed thereon” is directed to printed matter, and is thus entitled to no patentable weight. Regardless, the combination of Mullen-876 and Kobylkin renders the limitation obvious. SAMSUNG-1003, ¶111.

In the combination, Mullen-876 teaches that its dynamic credit card has a thin shaped body. SAMSUNG-1003, ¶112. For example, per Mullen-876, the dynamic credit card is “utilized using traditional infrastructure” such as “credit card reader[s].” SAMSUNG-1004, [0065]. Mullen-876 further describes that the dynamic credit card can be used to “make purchases that require the card to be *swiped*” (*i.e.*, so that information on the magnetic stripe is read by the credit card reader). *Id.* A POSITA would have understood or at least found it obvious that the dynamic credit card of Mullen-876 has a thin shaped body enabling it to be swiped

through a “traditional” credit card reader. SAMSUNG-1003, ¶112; *see, e.g.*, SAMSUNG-1004, Abstract, [0009] (“An encoder may also be provided such that *the number* is not only displayed to a user, but *may be written onto the magnetic stripe of the credit card such that traditional readers may read the credit card.*”), [0065].

Mullen-876 further teaches that the dynamic credit card has no fixed payment numbers disposed thereon. SAMSUNG-1003, ¶113. As previously discussed, the dynamic credit card generates “a secure credit card number (*e.g.*, a secret/hidden credit card number)...based on a timing signal (*e.g.*, an internal counter) to provide a *dynamic credit card number.*” SAMSUNG-1004, Abstract. Per Mullen-876, the “dynamic credit card number *may change continually or periodically* (*e.g.*, every sixty seconds) such that credit card numbers may not be copied by thieves and used at later times.” *Id.*, Abstract. Because the dynamic credit card number changes and is not fixed, the dynamic credit card number is “displayed to a user via a display,” rather than being physically printed on the card. *See id.*, Abstract, [0049], [0050]. FIG. 16 from Mullen-876 shows an example dynamic credit card having no fixed payment numbers disposed thereon, with the dynamic credit card number (outlined in red) displayed on the display screen (shown in yellow):



SAMSUNG-1004, Detail of FIG. 16 (annotated)

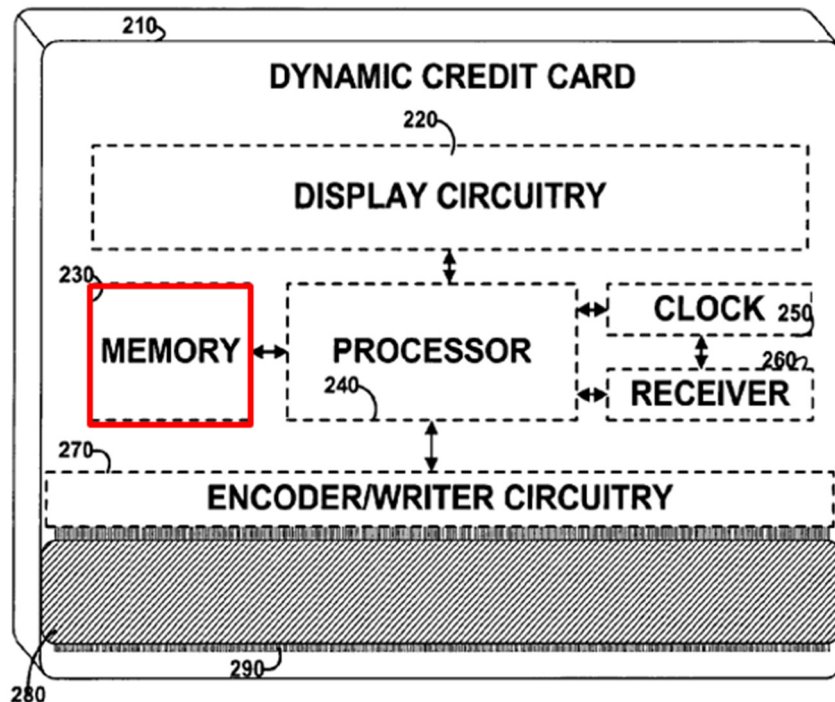
As another example, Mullen-876 teaches that the “credit card number may be updated continually in real time” such that the dynamic credit card would “not include a display.” SAMSUNG-1004, [0016]. The dynamic information is instead dynamically encoded on a magnetic strip, and a POSITA would have understood that there would be no need to present payment numbers to a user (e.g., for online transactions) in the case where dynamic numbers are continually updated in real time since any dynamic number displayed would be stale by the time the user reviewed it and static numbers are not used for payment transactions with Mullen-876’s device. *Id.*, [0070]; SAMSUNG-1003, ¶114

Further, in the combination, Kobylkin describes a “*payment card*” that “*can be a substantially blank card,*” and “*can lack any information,* such as the user’s name, *thereon.*” SAMSUNG-1005, [0017]. As previously discussed (*see* Sections

III.A.3-4, *supra*), it would have been obvious to a POSITA to modify the dynamic credit card of Mullen-876 to omit all fixed payment information from the front of the card, as taught by Kobylkin. SAMSUNG-1003, ¶¶115-116.

Element [1.2]

Mullen-876 describes, and the combination renders obvious, that the dynamic credit card includes a “memory 230,” as shown in FIG. 2. SAMSUNG-1004, [0076]; SAMSUNG-1003, ¶¶117-118:

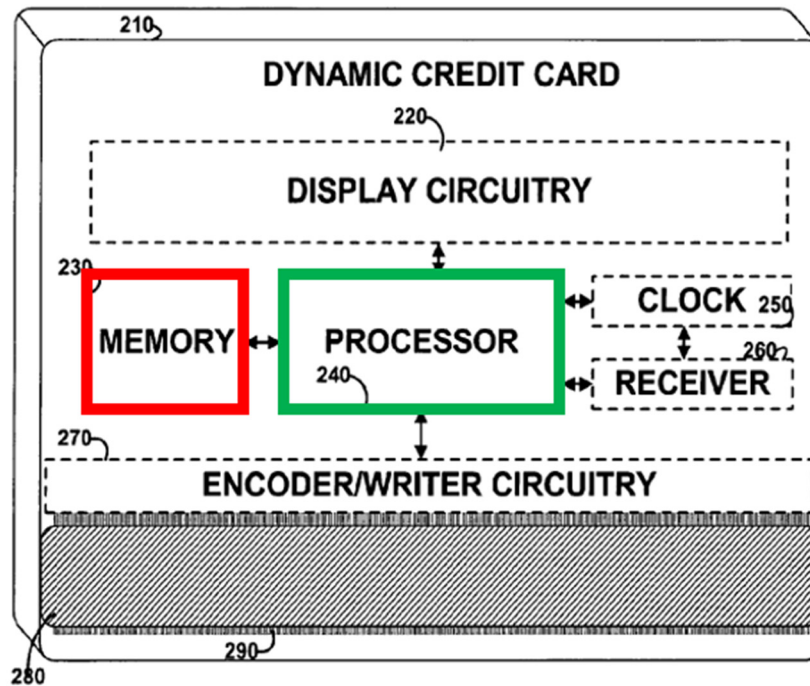


SAMSUNG-1004, Detail of FIG. 2 (annotated)

Element [1.3]

Mullen-876 describes, and the combination renders obvious, that the dynamic credit card includes a “processor 240” coupled to the “memory 230,” as

shown in FIG. 2. SAMSUNG-1004, [0076]; SAMSUNG-1003, ¶¶119-121:

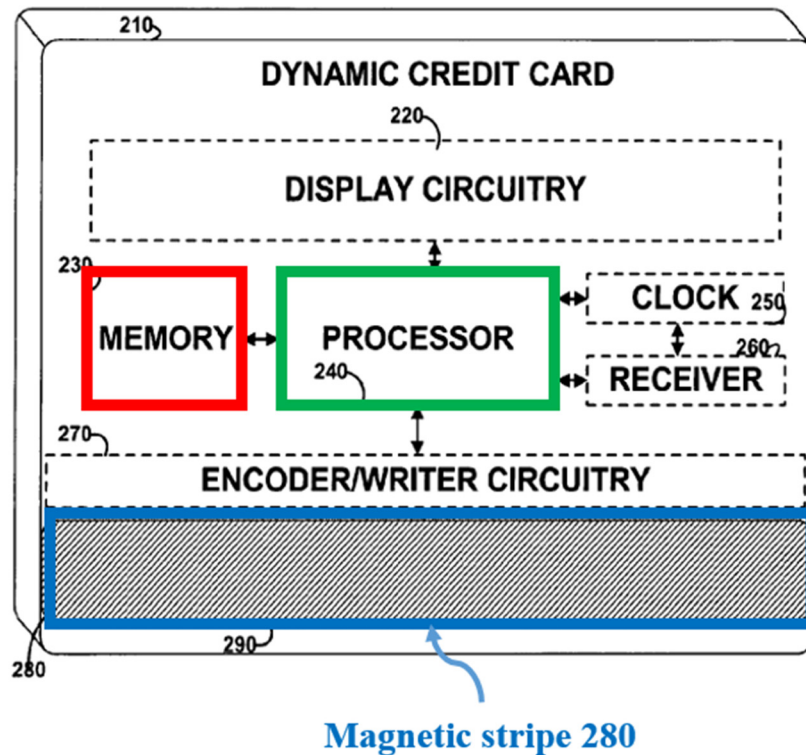


SAMSUNG-1004, Detail of FIG. 2 (annotated)

The dynamic credit card “encrypt[s]” the dynamic credit card number using an “encryption algorithm.” *See* SAMSUNG-1004, [0072], [0073]; *see also* FIG. 1 (“portion 150” showing encryption and decryption operations performed on the dynamic credit card number), [0097], [0102], [0103]. A POSITA would have understood or at least found it obvious that such an “encryption algorithm” would be executed by the “processor 240” of the dynamic credit card; Mullen-876 thus provides at least as much (if not more) detail regarding a cryptographic processor as the specification of the ’820 patent itself. SAMSUNG-1003, ¶120; *see, e.g.*, SAMSUNG-1004, [0072], [0073], [0097], [0102], [0103], FIG. 1.

Element [1.4]

Mullen-876 describes, and the combination renders obvious, a reader interface of the dynamic credit card in the form of a “magnetic stripe 280,” as shown in FIG. 2. SAMSUNG-1004, [0076]; SAMSUNG-1003, ¶¶122-124:



SAMSUNG-1004, Detail of FIG. 2 (annotated)

Mullen-876 describes that the dynamic credit card number (and other information) is written to the magnetic stripe “such that the number may be read by conventional credit card readers,” thereby rendering obvious that the magnetic stripe is a “reader interface.” See SAMSUNG-1004, [0105]; see also [0122]; SAMSUNG-1003, ¶123.

Element [1.5]

As previously discussed (*see* [1.4], *supra*), Mullen-876 describes that the dynamic credit card includes a reader interface (*e.g.*, magnetic stripe 280) that conveys a “dynamic credit card number” to “conventional credit card readers” to initiate payment transactions. *See* SAMSUNG-1004, [0105]; SAMSUNG-1003, ¶125; *see also* [0009].

Mullen-876 further teaches, and the combination renders obvious, that the dynamic credit card number comprises limited-use payment information. For example, Mullen-876 describes that the dynamic credit card number may be “*limited to only one use* and, as such, that a dynamic number (*e.g.*, *a dynamic credit card number* or verification code) *may not repeat for the life of a dynamic credit card* (*e.g.*, 1 to 5 years).” *See* SAMSUNG-1004, [0121]; *see also* [0062]; SAMSUNG-1003, ¶126. Mullen-876 describes that the number of uses for a particular dynamic credit card number can vary. *See, e.g.*, SAMSUNG-1004, [0071] (describing a dynamic credit card number that “may be invalidated at the facility if, for example, any particular number is used more than a particular number of times (*e.g.*, more than 10 times)”); SAMSUNG-1003, ¶¶126-128.

Element [1.6]

Mullen-876 describes, and the combination renders obvious, that the “dynamic credit card number” (*i.e.*, the limited-use payment information) is “utilized to represent a credit card number” in order to provide “increased

security.” SAMSUNG-1004, [0090]; *see also* [0024] (a “credit card authorization facility” receives and “decodes the dynamic credit card number ... to the secure credit card number”), [0068] (a “credit card processing facility ... may authorize payment by determining if the” dynamic credit card number “was valid for the time period” in which it was received); SAMSUNG-1003, ¶¶129-131.

(b) **Claim 2**

Element [2.0]

As previously discussed (*see* Section, I.C, *supra*), the limitation “comprises fixed payment information disposed thereon” is directed to printed matter, and is thus entitled to no patentable weight. Regardless, the combination of Mullen-876 and Kobylkin renders the limitation obvious. SAMSUNG-1003, ¶¶132-134.

In the combination, Mullen-876 describes that its dynamic credit card has the card-holder’s name disposed thereon. For example, Mullen-876 describes that “information about the particular user may be pressed/printed into the faceplate (*e.g., the name of the user*) and the faceplate may be fixed to the card after programming.” SAMSUNG-1004, [0094]; SAMSUNG-1003, ¶35.

Also in the combination, Mullen-876 describes that its dynamic credit card has a card payment network logo disposed thereon. For example, Mullen-876 describes that “the type of the credit card may be static (*e.g., printed on a credit card*) such that the type of the credit card does not change.” SAMSUNG-1004,

[0109]; *see also* [0102]. “Such a type may be indicative of a dynamic credit card (e.g., a dynamic credit card, *a Visa dynamic credit card*, or *an American Express dynamic credit card*)[.]” *Id.*; SAMSUNG-1003, ¶136.

Also in the combination, Kobylkin describes a payment card with a payment issuing logo disposed thereon. For example, Kobylkin describes an “instant disposable payment card,” and 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]; *see also* [0029]; SAMSUNG-1003, ¶137. As described above (*see* Sections III.A.3-4, *supra*), it would have been obvious to a POSITA to print or dispose information, such as the “logo of the provider” described in Kobylkin, on the dynamic credit card of Mullen-876. SAMSUNG-1003, ¶¶137-138.

Element [2.1]

See [1.1], *supra* (Kobylkin describes a “payment card” that “can be a substantially blank card,” and “can lack any information, such as the user's name, thereon.” SAMSUNG-1005, [0017]). SAMSUNG-1003, ¶¶139-141.

(c) Claim 6

Element [6.0]

Mullen-876 describes, and the combination renders obvious, that “[l]ocation information, or any information, may also be embedded into a dynamic number such that feedback can occur when a card is used online.” SAMSUNG-1004,

[0082]. Mullen-876 teaches that this information is used to detect fraudulent online transactions. For example, Mullen-876 describes that “a card may be stolen and may generate a number in Maryland, but may be used to buy an item on *an online store* by an accomplice located in Florida.” *Id.* Based on the embedded location information in the dynamic credit card number, “a processing/authorization facility (which may be the online store) may determine that the number was generated in Maryland (by retrieving the embedded location information) and may alert the Maryland authorities or *decline the transaction* because the IP address of the purchasing computer was located in Florida (not Maryland).” *Id.*; SAMSUNG-1003, ¶¶142-146.

(d) **Claim 10**

Element [10.0]

As previously discussed (*see* [1.5], *supra*), in the combination, Mullen-876 describes that the dynamic credit card number may be “*limited to only one use* and, as such, that a dynamic number (e.g., a dynamic credit card number or verification code) may not repeat for the life of a dynamic credit card (e.g., 1 to 5 years).” See SAMSUNG-1004, [0121]; *see also* [0019]-[0020] (describing a “counter” that increments with each use), [0062], [0071]; SAMSUNG-1003, ¶¶147-150.

Mullen-876 further describes that the dynamic credit card number is

generated cryptographically and dynamically by the processor using a timing signal such as a counter and a private key. *See* [1.3], *supra*. For example, per Mullen-876, the processor of the dynamic credit card “encrypt[s]” the dynamic credit card number using an “encryption algorithm” that involves a cryptographic combination of a card device transaction sequence count (e.g., a “counter”) and device secret keys (e.g., “private keys” stored on the device). *See* SAMSUNG-1004, [0019], [0053], [0057]-[0059], [0071]-[0073]; *see also* FIG. 1 (“portion 150” showing encryption and decryption operations performed on the dynamic credit card number), [0097], [0102], [0103]; SAMSUNG-1003, ¶149.

Element [10.1]

In the combination, Mullen-876 describes that the dynamic credit card includes “a counter” that is “increased after every purchase” and represents the “the number of transactions” that have been performed. SAMSUNG-1004, [0071]; SAMSUNG-1003, ¶¶151-153.

B. [GROUND 1B]: Claims 3-5 and 7-8 are obvious over Mullen-876, Kobylkin, and Patel

1. Overview of Patel

Patel describes that a “credit card, debit card, or other similar financial instrument is disclosed with the temporary assignment of a dynamic CVV for increased card security.” SAMSUNG-1014, Abstract. “The dynamic CVV is read, changed, and rewritten to the card with each transaction.” *Id.*

For example, Patel describes that “[t]o pay for the goods or services, the user 110 interacts with the transaction device 130,” such as by “the card 120 into a magnetic card reader 130 or placing an RFID-equipped card near transaction device 130.” *Id.*, [0057]. “The transaction device 130 reads the card data structure 310 from the card 120, and transmits verification data, including the dynamic CVV 330, across the network 140 to the financial institution 150” (*i.e.*, the card issuing authority). *Id.*, [0058]. Patel describes that the “financial institution 150 then authenticates the verification data, including the dynamic CVV 330, and transmits a verification code, including a new dynamic CVV 330 to the transaction device 130.” *Id.*, [0059]. “The transaction device 130 reads the new dynamic CVV 330, and writes the new CVV 330,” which was received from the card issuer, “to the magnetic strip 220” of the payment card. *Id.*, [0060]. “The financial institution 150 may then update its database to expire the previous dynamic CVV 330, and enter the new dynamic CVV 330 as the valid dynamic CVV 330.” *Id.*, [0062]. Patel stresses that “[o]nce the new CVV 330 has been provided, the old CVV 330 expires and is no longer valid.” *Id.*, [0065]; SAMSUNG-1003, ¶¶98-100.

2. The combination of Mullen-876, Kobylkin, and Patel

In the present combination, the dynamic credit card of the prior Mullen-876+Kobylkin combination is modified to implement the “dynamic CVV” techniques described in Patel, such that, each time the dynamic credit card is

swiped to perform a payment transaction, the current dynamic CVV is replaced on the magnetic stripe with a new dynamic CVV provided by the remote financial institution that verified the transaction. SAMSUNG-1003, ¶¶154-160; *see, e.g.*, SAMSUNG-1004, Abstract, [0049], [0121], FIG. 16; SAMSUNG-1005, [0015]-[0018]; SAMSUNG-1014, Abstract, [0057]-[0063], [0065].

3. Reasons to combine Mullen-876, Kobylkin, and Patel

A POSITA would have been motivated and found it obvious to implement Patel's dynamic CVV techniques in the Mullen-876+Kobylkin device. SAMSUNG-1003, ¶157. The Mullen-876+Kobylkin device already utilizes dynamic CVV codes. *See, e.g.*, SAMSUNG-1004, [0020]. Patel's particular dynamic CVV techniques, in which the dynamic CVV value is replaced by a new dynamic CVV value from the verifying financial institution at the conclusion of each transaction, would have enhanced the security and fraud resistance of the Mullen-876+Kobylkin system. SAMSUNG-1003, ¶157; *see, e.g.*, SAMSUNG-1014, Abstract, [0057]-[0063], [0065]. A POSITA would have understood fraud detection to be an important consideration in financial transactions, and thus would have been motivated to perform the combination to take advantage of these benefits. *See id.*; SAMSUNG-1003, ¶157.

Further, a POSITA would have found it obvious to modify Mullen-876+Kobylkin based on Patel's teachings because doing so entails the use of

known solutions to improve similar systems and methods in the same way. *KSR*, 550 U.S. at 417. A POSITA would have recognized that applying Patel's teachings to augment the Mullen-876+Kobylkin device would have led to predictable results without significantly altering or hindering the functions performed by the Mullen-876+Kobylkin device. SAMSUNG-1003, ¶158.

Moreover, a POSITA would have been motivated to incorporate the well-known techniques of Patel into Mullen-876+Kobylkin to achieve the predictable benefits described in Patel. SAMSUNG-1003, ¶159; *see, e.g.*, SAMSUNG-1014, Abstract, [0057]-[0063], [0065]. Indeed, a POSITA would have had a reasonable expectation of success implementing Patel's teachings in the context of Mullen-876+Kobylkin, because Mullen-876 contemplates the use of dynamic CVV codes like those used in Patel. *See* SAMSUNG-1004, [0020]; SAMSUNG-1014, [0057]-[0063], [0065]; SAMSUNG-1003, ¶¶159-160.

4. Analysis

(a) Claim 3

Element [3.0]

Mullen-876 describes, and the combination renders obvious, that the dynamic credit card number (*i.e.*, limited-use payment information) is conveyed via the magnetic-stripe and is unique to the payment device and to the magnetic stripe. SAMSUNG-1004, [0062], [0105], [0121]-[0122]; SAMSUNG-1003, ¶¶161-163.

Element [3.1]

Mullen-876 describes, and the combination renders obvious, that the limited-use payment information is limited to use by the payment device and is operable for conveying payment information to a magnetic-stripe payment card reader. SAMSUNG-1004, [0105]; *see also* [0009], [0062], [0072], [0121]-[0122]; SAMSUNG-1003, ¶¶164-166.

Element [3.2]

Mullen-876 describes, and the combination renders obvious, that the “dynamic credit card number” (*i.e.*, the limited-use payment information) has a limited period of valid use. SAMSUNG-1004, [0022], [0068]; SAMSUNG-1003, ¶¶167-168; *see also id.*, SAMSUNG-1014, [0015].

Element [3.3]

In the combination, Patel and Mullen-876 both describe and render obvious that the limited-use payment information is not valid when used other through a magnetic stripe payment card reader. SAMSUNG-1014, Abstract (“a static CVV may also be provided for manual entry”), [0057]-[0058], [0071]-[0074]; SAMSUNG-1004, [0082], [0122]. SAMSUNG-1003, ¶¶169-172.

(b) Claim 4

Element [4.0]

In the combination, Patel describes that a “credit card, debit card, or other similar financial instrument is disclosed with *the temporary assignment of a*

dynamic CVV for increased card security.” SAMSUNG-1014, Abstract. “The dynamic CVV is *read, changed, and rewritten to the card with each transaction.*” *Id.*; SAMSUNG-1003, ¶¶173-177.

For example, Patel describes that “[t]o pay for the goods or services, the user 110 interacts with the transaction device 130,” such as by “the card 120 into a magnetic card reader 130 or placing an RFID-equipped card near transaction device 130.” *Id.*, [0057]. “The transaction device 130 reads the card data structure 310 from the card 120, and transmits verification data, including *the dynamic CVV 330*, across the network 140 to the financial institution 150” (*i.e.*, the card issuing authority). *Id.*, [0058]. Patel describes that the “financial institution 150 then authenticates the verification data, including the dynamic CVV 330, and *transmits a verification code, including a new dynamic CVV 330 to the transaction device 130.*” *Id.*, [0059]. “The transaction device 130 reads the new dynamic CVV 330, and *writes the new CVV 330,*” which was received from the card issuer, “to the magnetic strip 220” of the payment card. *Id.*, [0060]. “The financial institution 150 may then update its database to *expire the previous dynamic CVV 330*, and enter the new dynamic CVV 330 as the valid dynamic CVV 330.” *Id.*, [0062]. Patel is clear that “[o]nce the new CVV330 has been provided, the old CVV 330 expires and is no longer valid.” *Id.*, [0065]; SAMSUNG-1003, ¶175.

Each dynamic CVV that is written to the magnetic strip of the card is

limited-use payment information provided by a card issuing authority, because it is 1) limited to a single use (because it will be expired when the next transaction is performed), and 2) transferred from the financial institution (card issuing authority) back to the transaction device 130, and then written to the card. SAMSUNG-1003, ¶176; *see, e.g.*, SAMSUNG-1014, [0057]-[0063], [0065], [0066] (“the dynamic CVV 230 will be valid only once”).

Element [4.1]

Patel describes that “*if a card 120 is not successfully updated with the new CVV 330...the attempted transaction ... fails.*” SAMSUNG-1014, [0063]. For example if the card information was entered manually and not presented to the transaction device 130 (i.e., payment card reader) via the magnetic strip, the transaction device 130 would not be able to update the magnetic strip, and the transaction would be rejected as invalid. SAMSUNG-1003, ¶¶178-180; *see, e.g.*, SAMSUNG-1014, [0057]-[0063]. Patel describes that “[t]his prevents a malicious actor from successfully completing several transactions by transmitting the old dynamic CVV 330 and then declining to transmit the success code.” SAMSUNG-1014, [0063].

(c) Claim 5

Claim 5 recites nothing that further limits or defines the claimed “payment device,” and is thus entitled to no patentable weight. Nonetheless, Mullen-

876+Kobylkin+Patel render the claim obvious even if it were afforded weight.

Element [5.0]

Mullen-876 describes that the processing facility receives with a transaction request information including account identification information, location information, and dynamic credit card information including the dynamic number and expiration date. SAMSUNG-1004, [0054]; [0118]; [0097]; SAMSUNG-1003, ¶¶181-183; *see also* SAMSUNG-1005, [0038], [0041].

Element [5.1]

In the combination, Patel describes that in payment transactions where the card is presented to a transaction device, the transaction succeeds if the dynamic CVV (*i.e.*, limited-use payment information) is authenticated as the current CVV. SAMSUNG-1014, [0057]-[0060]. Patel describes that if the card information was entered manually and not presented to the transaction device 130 (*i.e.*, payment card reader) via the magnetic strip, the transaction device 130 would not be able to update the magnetic strip with the current dynamic CVV, and the transaction would be rejected as invalid. SAMSUNG-1014, [0063]; *see also* [0057]-[0063]. Mullen-876 also describes that in some cases where a card is used online (*i.e.*, card-not-present transaction), location information associated with the card use for the transaction (*i.e.*, payment card reader information) is transmitted for security purposes. Thus, the Mullen-876+Kobylkin+Patel combination renders obvious a

transaction where the card is present and transmits a valid dynamic CVV having been updated by the transaction device (*i.e.*, valid payment card reader information), and further renders obvious a transaction where the card is not present (online transaction) and an outdated dynamic CVV is presented (*i.e.*, invalid payment card reader information). SAMSUNG-1003, ¶¶184-185.

Element [5.2]

In the combination, Patel describes that a transaction at a transaction device is approved where the dynamic CVV is authenticated at a financial institution. SAMSUNG-1014, [0058]; [0059]; SAMSUNG-1003, ¶¶186-187.

Element [5.3]

In the combination, Mullen-876 describes that in transactions where the dynamic credit card is not present (*e.g.*, online shopping and manual entry transaction), based on embedded location information in the dynamic credit card number, “***a processing/authorization facility (which may be the online store)*** may determine that the number was generated in Maryland (by retrieving the embedded location information) and may alert the Maryland authorities or ***decline the transaction*** because the IP address of the purchasing computer was located in Florida (not Maryland).” SAMSUNG-1004, [0082]; SAMSUNG-1003, ¶¶188-189.

Element [5.4]

In the combination, Patel describes that in a transaction where the card is not

present, (e.g., online shopping and manual entry transaction), the static CVV must be used. SAMSUNG-1014, [0059]. Where an incorrect dynamic CVV is provided with the payment information, Patel describes that the financial institution can reject the transaction. SAMSUNG-1014, [0063] (“*if a card 120 is not successfully updated with the new CVV 330*, the old CVV 330 may remain valid [but] *the attempted transaction still fails*”); *see also* [0057]-[0063]; cl. [8]; SAMSUNG-1003, ¶¶190-192.

(d) **Claim 7**

Element [7.0]

Patel describes, and the combination renders obvious, approval of a transaction where the dynamic CVV is authenticated by the financial institution, but a transaction not at a transaction device (e.g., online transaction) involving the dynamic CVV may be declined. SAMSUNG-1014, [0072], [0063]; *see also* [0057]-[0063]; SAMSUNG-1003, ¶194. A POSITA would have understood that Patel provides that the financial institution (e.g., card issuing authority) would decline manual entry/online transactions that attempt to use the dynamic CVV in place of the static CVV for security reasons. SAMSUNG-1014, [0072], [0076]; SAMSUNG-1003, ¶¶193-195.

Element [7.1]

In the combination, Mullen-876 describes that the dynamic credit card number is valid within a time period, and declines a use of the dynamic credit card

where the number is expired. SAMSUNG-1004, [0068]; [0013]; *see also* [0011], [0022]; SAMSUNG-1003, ¶¶ 196-198 (citing SAMSUNG-1014, [0015]).

Element [7.2]

In the combination, Patel describes that the user of the card can provide verification of the transaction when required to complete the transaction. SAMSUNG-1014, [0077]. A user provides verification of a card transaction (*e.g.*, approves), or does not verify the transaction (*e.g.*, denies an approval) in order for the financial institution to approve or deny the transaction processing. SAMSUNG-1003, ¶¶ 199-200.

Element [7.3]

Mullen-876 describes a “dynamic credit card” that is operable to encode “a secure credit card number (*e.g.*, a secret/hidden credit card number)...based on a timing signal (*e.g.*, an internal counter) to provide a dynamic credit card number.” SAMSUNG-1004, Abstract. Mullen-876 describes that the dynamic credit card number (and other information) is written to the magnetic stripe “such that the number may be read by conventional credit card readers” in place of the assigned card issuer information. SAMSUNG-1004, [0105]; *see also* [0122]; SAMSUNG-1003, ¶¶ 202-204. The financial institution limits the use of the dynamic credit card number to use in place of the secure credit card number issued by the card issuer for payment transactions using the dynamic credit card. SAMSUNG-1003, ¶ 202.

(e) **Claim 8**

Element [8.0]

In the combination, Mullen describes that the magnetic stripe can receive and transmit transaction information wirelessly, and that the dynamic credit card can include user identification information. SAMSUNG-1004, [0027], [0105]; SAMSUNG-1003, ¶¶205-209. Additionally, in the combination, Patel describes that a user may be required to input additional information to verify their identity. SAMSUNG-1014, [0006]; SAMSUNG-1003, ¶206.

Element [8.1]

In the combination, Patel describes that a user may be required to input information to verify their identity, including personalized security information and passwords. SAMSUNG-1014, [0006]. Patel describes that the user verification input can be input through an input device such as a stylus pad, touch screen, or telephone. SAMSUNG-1014, [0031]; SAMSUNG-1003, ¶¶208-209.

Element [8.2]

In the combination, Mullen-876 describes that the dynamic credit card can include a display including a display of transaction information such as credit card number, security code, expiration date, or transaction notifications. SAMSUNG-1004, Abstract, [0018]; [0021], [0092], Abstract; SAMSUNG-1003, ¶¶210-211.

Element [8.3]

In the combination, Patel describes that the user can provide verification of

the transaction (*i.e.*, payment approval authorization) when required in order to complete the transaction. SAMSUNG-1014, [0077]. A user provides verification of a card transaction (*e.g.*, approves), or does not verify the transaction (*e.g.*, denies an approval) in order for the financial institution to approve or deny the transaction processing. SAMSUNG-1003, ¶¶212-214.

C. [GROUND 1C]: Claim 9 is obvious over Mullen-876, Kobylkin, and Smith

1. Overview of Smith

In the combination, 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-1006, 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., SAMSUNG-1006, [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]; SAMSUNG-1003, ¶¶86-88.

2. The combination of Mullen-876, Kobylkin, and Smith

In the present combination, the dynamic credit card of the prior Mullen-876+Kobylkin combination of Ground 1A is further modified so that the static credit card number conveyed by the dynamic credit card in payment transactions along with a dynamic security code is a credit card number like Smith’s MCA that has been substituted for a real card account number like Smith’s RCA. SAMSUNG-1004, [0021], [0028]; SAMSUNG-1006, [0034]; *see also id.*, [0035]-[0040], [0066]-[0073], FIG. 6; SAMSUNG-1003, ¶¶215-219. Further, as taught in Smith, the static credit card number (e.g., MCA) can be provisioned to the payment device from a card issuing authority. SAMSUNG-1006, [0052]-[0059], FIGS. 4A-4B (MCA provisioning); *see also id.*, [0037] (“service provider 110 ... may be operated by or on behalf of the issuer 112”), [0064] (“issuer 112 provides the MCA”) SAMSUNG-1003, ¶216.

3. Reasons to combine Mullen-876, Kobylkin, and Smith

A POSITA would have found it obvious and would have been motivated to implement the dynamic credit card in the combination to use a static substituted card number (e.g., like Smith’s MCA) “to more securely conduct a contactless

payment transaction.” SAMSUNG-1006, [0040]; SAMSUNG-1003, ¶217.

Transaction security would be improved in the device of the resulting combination since the real card number would not be conveyed to a merchant in a transaction, thereby significantly reducing opportunity for the real card number to be skimmed or accessed by unauthorized entities. *Id.* The security of the payment card would also be improved since the real card number would not need to be stored on the card. SAMSUNG-1006, [0034]; SAMSUNG-1003, ¶217.

Provisioning Mullen-876’s dynamic credit card with the static substituted card number from a card issuing authority as taught in Smith also would have been obvious, and a POSITA would have been motivated to modify the dynamic credit card in this manner to ensure the substituted card number is obtained from a trusted source (*i.e.*, the issuer) that could suitably coordinate with a service provider to map the substituted number to the user’s actual card number for use in validating transactions involving the substituted card number. SAMSUNG-1006, [0069]-[0073], FIG. 6; SAMSUNG-1003, ¶218.

Further, a POSITA would have found it obvious to modify Mullen-876+Kobylkin based on Smith’s teachings since doing so entails the mere use of known solutions to improve similar systems and methods in the same way. *KSR*, 550 U.S. at 417. A POSITA would have had a reasonable expectation of success implementing the combination, especially since Mullen-876 and Smith similarly

describe mobile payment devices that use substituted and/or dynamically generated parameters in payment transactions. SAMSUNG-1003, ¶219.

4. Analysis

(a) Claim 9

Element [9.0]

In the combination, Mullen-876 describes a dynamic security code (*i.e.*, a dynamically-generated one-time limited use payment information portion) generated by a processor of the dynamic credit card. SAMSUNG-1004, [0021], [0028], [0009] (“changes after each use”), [0071] (“counter may be increased after every purchase”), [0019]-[0022], [0076], [0080], [0085]. Mullen-876’s dynamic numbers are generated when coupled to a reader interface accessible to the processor. For example, Mullen-876 explains that “the counter is increased when a number is used.” *Id.*, [0071]. Mullen-876 also explains information about the card’s current state, such as the card’s location, at the time of the transaction can be embedded in a dynamically generated number. *Id.*, [0081]-[0082]. The dynamic card can also receive data from the reader interface regarding “dynamic coding information/schemes” for use in generating a dynamic number in a transaction. *Id.*, [0120]; SAMSUNG-1003, ¶¶220-222.

Element [9.1]

Mullen-876 discloses that the payment information conveyed to a payment card reader, at the time of transaction, can include a static credit card number (*i.e.*,

a static limited-use portion) and a dynamic security code (*i.e.*, a dynamically-generated limited-use portion). SAMSUNG-1004, [0021], [0028]. In the combination, Smith teaches that the static credit card number such as an MCA can have an expiration date and limited use. SAMSUNG-1006, [0086]; SAMSUNG-1003, ¶¶223-225.

Element [9.2]

In the combination, Smith teaches that the static credit card number can be a substituted credit card number such as an MCA that is provided by a card issuing authority for use in place of a real credit card number such as an RCA (*i.e.*, a card issuer payment information). SAMSUNG-1006, [0034], [0052]-[0059], FIGS. 4A-4B (MCA provisioning); *see also id.*, [0037] (“service provider 110 ... may be operated by or on behalf of the issuer 112”), [0064] (“issuer 112 provides the MCA”) SAMSUNG-1003, ¶¶226-228.

D. [GROUND 2A]: Claims 11, 12, 15, 16-18, and 20 are obvious over Smith, Kobylkin, and Gomez

1. Overview of Gomez

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-1007, 5:14-18, Abstract; SAMSUNG-1003, ¶¶89-97.

2. The combination of Smith, Kobylkin, and Gomez

In the combination, the functionality of Smith's mobile device is extended to permit the mobile device to be used for the separate 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], [0088], [0134]. For example, the 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, ¶¶230-231.

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, ¶¶235; *see, e.g.*, SAMSUNG-1006, [0031]; SAMSUNG-1005, [0015]-[0018].

Also in the combination, the mobile device utilized in Smith's online payment system can implement a user credential check prior to generating a

payment cryptogram, based on the teachings of Gomez. SAMSUNG-1003, ¶¶236-237; *see, e.g.*, SAMSUNG-1007, 5:14-18.

3. Reasons to combine Smith, Kobylkin, and Gomez

A POSITA would have been motivated and found it obvious to configure the mobile device utilized in Smith’s online payment system to be used in activating and/or funding a disposable payment card like Kobylkin’s for multiple reasons. SAMSUNG-1003, ¶¶230-232. To start, a POSITA would have sought to extend the functionality of Smith’s mobile device according to the teachings of Kobylkin so that the user could make beneficial and convenient use of disposable payment cards. *Id.* Kobylkin itself describes a number of advantages associated with disposable payment cards, including that they can be “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].

The use of Smith’s mobile device to fund and/or activate Kobylkin’s disposable cards also would have been obvious since Kobylkin already contemplates that an ordinary mobile device—such as a smartphone like Smith’s—would be suitable to use in funding and/or activating disposable payment cards.

SAMSUNG-1006, [0033], [0004] (“NFC-capable mobile devices”); SAMSUNG-1005, [0031], [0050] (“user’s device has an NFC reader”), [0052] (“user smart phone”), [0134]. Indeed, it was well-known by the Critical Date of the ’820 patent that smartphones commonly included multiple applications and were typically multi-functional to allow a user to perform a range of tasks or activities from making phone calls to checking email, playing games, capturing photos/videos, browsing the web, making payments, and more. SAMSUNG-1003, ¶233. In this context, a POSITA would have found been driven to allow a user to perform Kobylkin’s activation and funding operations on the same mobile device used for other purposes such as making contactless payment transactions in Smith’s system, especially since using the same device for multiple tasks would have increased convenience to the user by not requiring the user to access different devices for Smith’s payment transactions and Kobylkin’s funding/activation of disposable cards. *Id.*

Further, a POSITA would have found it obvious to modify Smith’s mobile device 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, ¶234. “[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*, 550 U.S. at 417. A POSITA would have found that extending the functionality of Smith’s mobile device through integration of Kobylkin’s techniques would have led to predictable results without significantly altering or hindering the functions performed by Smith’s mobile device. SAMSUNG-1003, ¶234. 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, especially since similar mobile devices were used in the respective systems of Smith and Kobylkin individually, and such mobile devices were ordinarily designed to be multifunctional to support multiple apps, capabilities, and services. *Id.*

A POSITA would have been motivated and found it obvious to modify the payment cards in Smith’s online payment system to include only selected, non-confidential information on their face, as described in Kobylkin, by at least the same considerations previously described with respect to the Mullen-876 and Kobylkin combination. *See* Section III.A.4, *supra*; SAMSUNG-1003, ¶235.

In addition, a POSITA would have been motivated and found it obvious to implement a user credential check prior to Smith’s mobile device generating a payment cryptogram, based on the teachings of Gomez. SAMSUNG-1003, ¶236. Smith describes one of its aims as “reducing the potential for fraud” in payment transactions performed by its system. SAMSUNG-1006, [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, ¶236. Implementing Gomez’s credential checking 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, as taught by Gomez. SAMSUNG-1006, [0034], [0045]; SAMSUNG-1007, 5:14-18; SAMSUNG-1003, ¶236.

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, ¶237. *KSR*, 550 U.S. at 417. 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, ¶237.

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-1006, [0034], [0045]; SAMSUNG-1007, 5:14-18; SAMSUNG-1003, ¶237.

Indeed, a POSITA would have had a reasonable expectation of success implementing Gomez’s teachings in the context of Smith’s mobile device, especially since Gomez and Smith each describe user payment devices similarly adapted for use in contactless payment transactions. *See* SAMSUNG-1006, [0033]; SAMSUNG-1007, 10:34-42 SAMSUNG-1003, ¶237.

4. Analysis

(a) Claim 11

Element [11.0]

The preamble is not limiting because it does not “recite[] essential structure or steps” and is not “necessary to give life, meaning, and vitality to the claim.” *Arctic Cat Inc. v. GEP Power Products, Inc.*, 919 F. 3d 1320, 1327 (Fed. Cir. 2019). However, to the extent the preamble is determined to be limiting, the combination renders it obvious.

In the combination, 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-1006, Abstract, [0029]-[0031], [0034], [0063]-[0065], FIG. 1; SAMSUNG-1003, ¶¶238-239.

As discussed in greater detail below (*see* [11.5], *infra*), 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.*, SAMSUNG-1006, [0033]. Before the Critical Date of the ’820 patent, it was well-known in the art that smart phones and tablet computers provided visual user-interfaces that enabled users to perform online transactions, such as purchasing items from websites by submitting payment information via an HTML form or other mechanism. *See, e.g.*, SAMSUNG-1008, [0007] (describes “provid[ing] a financial transaction Web service to Web enabled clients” such as smart phones and tablets); SAMSUNG-1009, Abstract, FIGS. 5-10; SAMSUNG-1010, FIG. 4, [0091]; SAMSUNG-1015, [0041]-[0042], [0045]; SAMSUNG-1003, ¶240.

In addition, the ’820 patent describes “online” transactions in its payment system as, for example, involving the transfer of payment details (e.g., via NFC) from a mobile computing device to a more full featured computer (e.g., a PC), which then uses the transferred payment details to make an online purchase (e.g., from a website). *See, e.g.*, SAMSUNG-1001, 12:50-13:19, 18:30-39, FIG. 5, FIG. 10. As described below, Smith’s mobile device is operable to transfer payment details to external devices via NFC, and thus is operable to perform the type of “online” transactions described in the ’820 specification and recited in the present claim. *See, e.g.*, SAMSUNG-1006, [0035], [0061], [0067]; *see* [11.9], *infra*.

Further, Smith's payment details (*e.g.*, the MCA and cryptogram, described below) are described as being used in the standard credit card network, and thus would have been suitable for online purchases like those described in the '820 patent. SAMSUNG-1003, ¶¶241-242; *see, e.g.*, SAMSUNG-1006, Abstract, [0029]-[0031], [0034], [0063]-[0065], FIG. 1; SAMSUNG-1007, Abstract, 5:7-18, 13:1-4, 14:3-7, 21:5-19 (describing a system similar to Smith's in which a substitute account number (*e.g.*, Smith's MCA) is used to "make purchases online"). Thus, in the combination, Smith teaches an "online payment system."

Element [11.1]

In the combination, Kobylkin describes a "***payment card*** ... made of paper, paperboard, card stock, plastic, or any other material." SAMSUNG-1005, [0101]. Kobylkin describes that a user of the payment card can "[s]wipe a magnetic strip of the payment card to facilitate payment for [a] purchase." *Id.*, [0015]; *see also* Abstract. For example, "the user can swipe the ... payment card at ***a POS device***." *Id.*, [0048]; *see also* Abstract. A POSITA would have understood that the payment card of Kobylkin must be at least as thin as a standard credit card in order for it to be "swiped" through the magnetic reader of a standard POS device (*e.g.*, a credit card reader). SAMSUNG-1003, ¶¶243-246; *see, e.g.*, SAMSUNG-1005, Abstract, [0015], [0048], [0101].

Kobylkin further describes that the payment card "***can be a substantially***

blank card,” and “*can lack any information,* such as the user's name, *thereon.*”

SAMSUNG-1005, [0017]. Thus, in the combination, Kobytkin teaches a thin payment card comprising no fixed payment numbers visible thereon.

In addition, as previously discussed (*see* Section I.C, *supra*), the limitation that the thin payment device have “no 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 is thus entitled to no patentable weight.

Element [11.2]

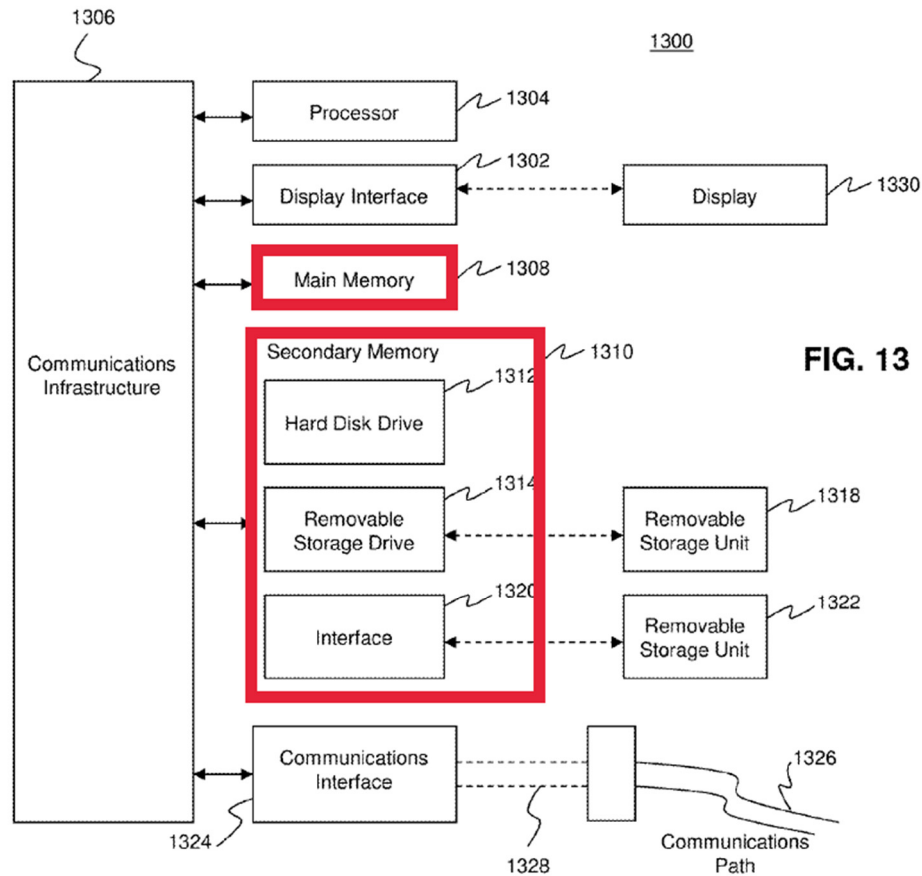
In the combination, Smith describes that its payment system includes a “*mobile device*” (*i.e.*, personal computing device) that can be “any type of mobile computing device... such as a cellular phone, smart phone, table computer, etc.” SAMSUNG-1006, [0033]. Smith further describes that the mobile device includes a “*processor.*” *See, e.g., id.*, [0042], [0104], [0108], FIG. 13); SAMSUNG-1003, ¶¶247-248.

Element [11.3]

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-1006, [0104], [0108]; SAMSUNG-1003,

¶¶249-250. FIG. 13 from Smith shows these components of the mobile device:

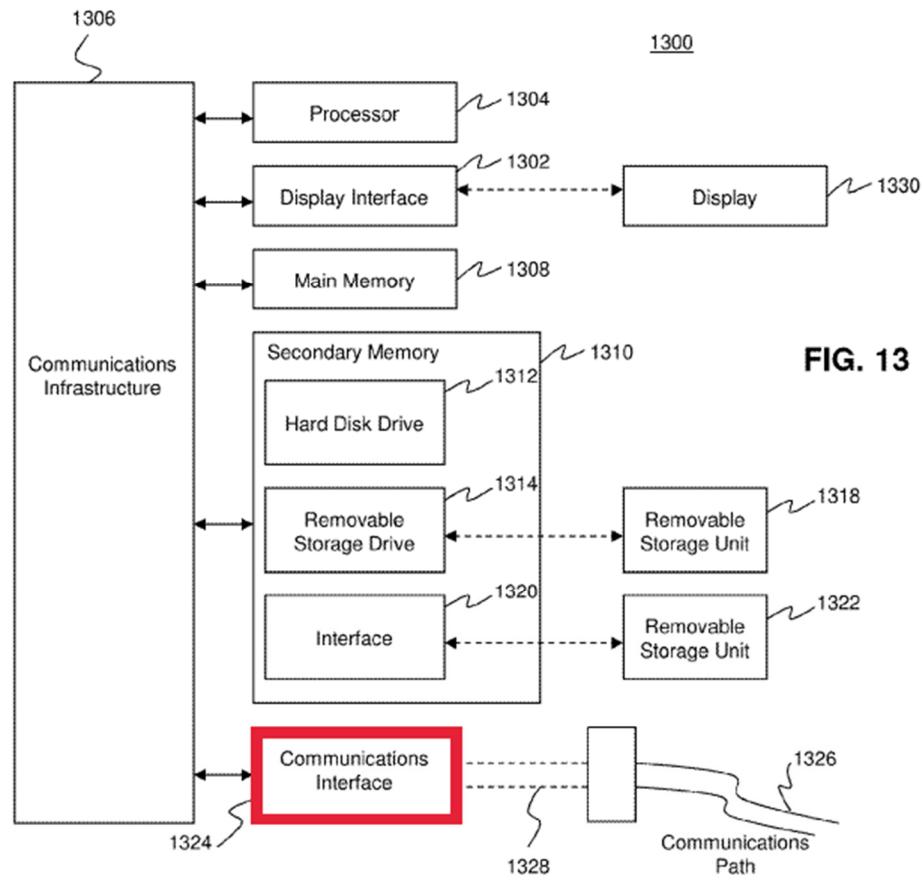


SAMSUNG-1006, FIG. 13 (annotated)

Element [11.4]

In the combination, Smith describes that the mobile device includes a wireless interface. For example, 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 ... *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, ¶¶251-252. FIG. 13 from Smith shows this component of the mobile device:

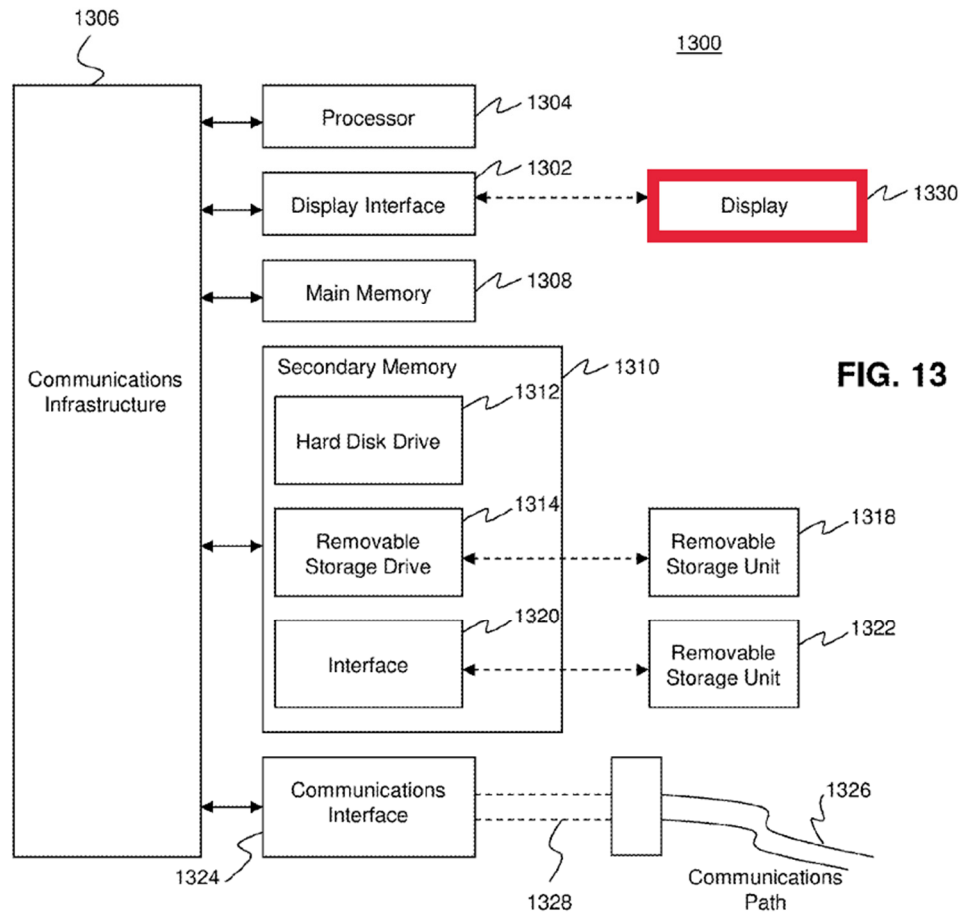


SAMSUNG-1006, FIG. 13 (annotated)

Element [11.5a]

In the combination, Smith describes that the mobile device includes a display. For example, Smith describes that the “mobile device ... may be implemented in the computer system 1300” shown in FIG. 13, which includes a

“display 1330.” SAMSUNG-1006, [0104], FIG. 13; *see also* [0055], [0059],
[0083], FIGS. 7-8; SAMSUNG-1003, ¶¶253-254:



SAMSUNG-1006, FIG. 13 (annotated)

Element [11.5b]

The combination of Smith, Kobylkin, and Gomez renders this limitation obvious in multiple ways. SAMSUNG-1003, ¶¶255-260.

First, in the combination, Smith describes that the mobile device 102 “may be any type of mobile computing device 102 suitable for performing the functions as disclosed herein as will be apparent to persons having skill in the relevant art,

such as a cellular phone, *smart phone, table computer*, etc.” SAMSUNG-1006, [0033]. Prior to the Critical Date of the ’820 patent, it was well-known in the art that smart phones and tablet computers provided visual user-interfaces that enabled users to perform online transactions, such as purchasing items from websites using by submitting payment information via an HTML form or other mechanism.

SAMSUNG-1003, ¶256; *see, e.g.*, SAMSUNG-1008, [0007] (describes “provid[ing] a financial transaction Web service to Web enabled clients” such as smart phones and tablets); SAMSUNG-1009, Abstract, FIGS. 5-10; SAMSUNG-1010, FIG. 4, [0091]. Thus, a POSITA would have understood or at least found it obvious that the display of Smith’s mobile device was operable to provide a visual user-interface operable for performing online transactions. SAMSUNG-1003, ¶256; *see, e.g.*, SAMSUNG-1006, [0033]; SAMSUNG-1008, [0007]; SAMSUNG-1009, Abstract, FIGS. 5-10; SAMSUNG-1010, FIG. 4, [0091].

Second, in the combination, Gomez describes displaying payment information on a display of a mobile device to enable a user to enter the payment information into a website payment form displayed on a PC. For example, Gomez describes that an “authentication cryptogram” (described in greater detail below) “may be displayed” by the mobile device “which may be beneficial in facilitating an online transaction.” SAMSUNG-1007, 13:1-4. The “authentication cryptogram ... is generated for each attempted use, and is preferably communicated in the

account name field (*i.e.*, of a magnetic stripe on the card, in a NFC transmission, ***using an online web page***, etc.) instead of the cardholder's actual name.” *Id.*, 14:3-7. Gomez further describes using its mobile device for “Online and Recurring Transactions,” stating that “[t]o make purchases online using an EPIC card, a customer may select ‘Epic Pay’ from the available payment methods shown on the vendor's web site, then ***enter his/her EPIC credentials (e.g., into an account authentication popup window)***.” *Id.*, 21:4-9; SAMSUNG-1003, ¶257.

Third, as discussed above, the ’820 patent describes “online” transactions in its payment system as involving the transfer of payment details (*e.g.*, via NFC) from a mobile computing device to a more full featured computer (*e.g.*, a PC), which then uses the transferred payment details to make an online purchase (*e.g.*, from a website). *See, e.g.*, SAMSUNG-1001, 12:50-13:19, 18:30-39, FIG. 5, FIG. 10. As described below (*see* [11.9], *infra*), Smith’s mobile device is operable to transfer payment details to external devices via NFC, and thus is operable to perform the type of “online” transactions described in the ’820 specification and recited in the present claim. SAMSUNG-1003, ¶258; *see, e.g.*, SAMSUNG-1006, [0035], [0042], [0061], [0067]. For example, Smith describes a visual interface (“payment UI 204”) that is operable to enable a user to select a particular MCA to use for an NFC transaction, where the payment details associated with the MCA are transferred via NFC to an external device. SAMSUNG-1003, ¶258; *see, e.g.*,

SAMSUNG-1006, [0042] (“mobile device 102 may also include a payment user interface (UI) 204....for management of a payment application 208”), [0045] (“a mobile cloud account [MCA] is selected by the user for the funding of the payment transaction” via the payment UI 204, and “[t]he user may then initiate transmission of the payment credentials ... to the contactless terminal 104 to initiate the transaction.”). Based on the ’820 patent’s specification, transferring the payment details via NFC to an external device is all that is required of the claimed personal computing in performing an “online transaction.” *See, e.g.*, SAMSUNG-1001, 12:50-13:19, 18:30-39, FIG. 5, FIG. 10.

Further, it was well-known in the art prior to the Critical Date that payment credentials could be transmitted via NFC to different types of devices, including PCs. *See, e.g.*, SAMSUNG-1011, [0004], [0017], [0020], FIG. 4; SAMSUNG-1012, [0028]. Thus, Smith’s “payment UI 204” was “operable for performing online transactions” as described in the ’820 patent. SAMSUNG-1003, ¶259.

Element [11.6]

As previously discussed (*see* [11.5], *supra*), in the combination, Smith describes that the mobile device includes “***a payment user interface (UI) 204...*** for management of a payment application 208... executed by a processor of the mobile device.” SAMSUNG-1006, [0042]. Smith further describes that the mobile device includes “an input device” including “at least one of: a mouse,

keyboard, click wheel, scroll wheel, and touch screen.” *Id.*, [0102]; SAMSUNG-1003, ¶¶261-262.

Element [11.7]

In the combination, Smith describes that the mobile device wirelessly obtains “***mobile cloud account data***” (*i.e.*, card device payment account information) when the “mobile cardlet” including the mobile cloud account data is provisioned “***over-the-air (OTA)***” (*i.e.*, wirelessly) to the mobile device. *See* SAMSUNG-1006, [0044]-[0045], [0048], [0050] (“the service provider 110 may push (e.g., transmit) the generated master key identifier and mobile cardlet to the mobile device 102” via “a mobile network operator (MNO) 304,” and “mobile device 102 may receive the data”); SAMSUNG-1003, ¶¶264-268.

In addition, Smith also teaches that the “mobile cloud account data” can be “provisioned” to the wallet of the mobile device, and Smith indicates that such “provisioning” can take place “over-the-air (OTA)” (*i.e.*, wirelessly). *See* SAMSUNG-1006, [0075]; SAMSUNG-1003, ¶266.

Smith further describes that the mobile cloud account data is transmitted to the mobile device with the post issuance script. *See* SAMSUNG-1006, [0058] (“The post issuance script may be configured to cause the mobile device 102 to transmit mobile cloud account data for a selected MCA from a database or storage in the mobile device 102 to the mobile cardlet inside of the secure element 210”),

[0059] (“the service provider 110 may transmit the post issuance script and related data” including the MCA “to the mobile device 102, which may receive the script and data in step 436”); SAMSUNG-1003, ¶¶267-268. Based at least on Smith’s disclosure of “over-the-air” provisioning, it would have been obvious to a POSITA that the mobile device would be operable to obtain the mobile cloud account data wirelessly. SAMSUNG-1003, ¶¶267-268; *see, e.g.*, SAMSUNG-1006, [0044]-[0050], [0058]-[0059].

Element [11.8]

In the combination, Smith describes “***generating...a payment cryptogram***” (*i.e.*, limited-use payment information) ***based on at least a portion of the mobile cloud account data 802***” (*i.e.*, the card device payment account information, *see* [11.7], *supra*). SAMSUNG-1006, [0103]; *see also* [0067]; SAMSUNG-1003, ¶¶269-272.

A POSITA would have understood or at least found it obvious that the payment cryptogram is limited-use. For example, Smith describes that the payment card device “generat[es]” a “payment cryptogram” each time a payment transaction is initiated. SAMSUNG-1006, [0099], [0103], FIG. 12 (description of generating the cryptogram is in the context of FIG. 12, which describes a process performed by the payment card device for a single transaction); SAMSUNG-1003, ¶270. A POSITA would have understood or at least found it obvious that a

different payment cryptogram value is generated for each transaction, because if the value of the cryptogram did not change it would simply be generated once and stored. *See id.* Thus, each generated cryptogram is limited to use in verifying the specific transaction for which it was generated. *See id.*

In addition, Smith describes that its “payment cryptogram may be...a ***dynamic card validation code.***” SAMSUNG-1006, [0103]. A POSITA would have understood that a “dynamic card validation code,” also referred to as a “***dCVV***,” was a well-known type of limited-use credential used for payment verification prior to the Critical Date. *See, e.g.,* SAMSUNG-1013, [0007] (a dCVV is a “***dynamically generate[d] ... verification value for each transaction*** which can be used to authenticate the transaction”), [0021]-[0022] (the dCVV is “generated on the payment device, embedded into the payment data, and transmitted to a point of sale terminal”), [0029]-[0031] (“***Each time the payment service is initiated, a dCVV is generated*** on the payment device for authentication purposes”); SAMSUNG-1003, ¶271.

Element [11.9]

In the combination, Smith describes that the payment card device is operable to transmit “***payment credentials***” (*i.e.*, complete payment information) “***via near field communication***” (*i.e.*, via the wireless interface, *see* [11.4], *supra*) “from the mobile device 102 to the contactless terminal 104.” SAMSUNG-1006, [0067].

Smith further describes that the “*payment credentials may include a payment cryptogram*” (*i.e.*, the limited-use payment information), which is “generated based on at least a portion of the mobile cloud account data.” *Id.*; SAMSUNG-1003, ¶¶273-274. A POSITA would have understood or at least found it obvious that the set of “payment credentials” described in Smith is “generated” for each transaction, because the payment card device assembles different pieces of payment information—some retrieved from storage (*e.g.*, the mobile cloud account number (MCA), some dynamically generated (*e.g.*, the payment cryptogram)—to form (*i.e.*, generate) the set of payment credentials to be transmitted via NFC. SAMSUNG-1003, ¶¶272-274; *see, e.g.*, SAMSUNG-1006, [0035], [0061], [0067].

Element [11.10]

In the combination, Smith describes that the “*payment cryptogram*” (*i.e.*, limited-use payment information) is used by a “service provider” to “*validate*” the payment transaction. *See* SAMSUNG-1006, [0096] (“a validation device may validate the payment cryptogram”), [0097]; SAMSUNG-1003, ¶¶275-278. Smith further teaches that a “*real card account*” or “RCA” may “correspond to a *payment account issued to the user by an issuer 112*,” thereby indicating that the RCA is “card issuer payment information.” SAMSUNG-1006, [0034]. Smith describes that by validating transactions based on the “payment cryptogram,” instead of or in place of the “RCA,” “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.*; *see also, e.g.* [0096]-[0097], [0103], claim 7; SAMSUNG-1003, ¶¶275.

It also would have been obvious and a POSITA would have understood that the “*payment cryptogram*” in the combination would be configured to be used in place of an issuer-provided card verification value such as a CVV2 or CVC2 value that would commonly be printed on the physical payment card (or a CVV1 or CVC1 value encoded into the magnetic stripe of the physical payment card) corresponding to the mobile cardlet stored in the mobile device of the combination. SAMSUNG-1003, ¶276; SAMSUNG-1006, [0031] (“payment card may be a physical card”), [0034]; *see also id.*, SAMSUNG-1015, [0003]-[0007]; SAMSUNG-1014, [0005]-[0006]. For example, the payment cryptogram would be used to validate a transaction conducted with a mobile cardlet as taught in Smith, while a well-known issuer-provided verification value would be used to validate a transaction conducted with a corresponding physical payment card (*e.g.*, an ordinary credit card). The payment cryptogram is thus used in place of the issuer-provided verification value assigned to the physical payment card. SAMSUNG-1003, ¶276.

(b) Claim 12

Element [12.0]

As previously discussed, in the combination, Kobylkin describes that the thin payment device bears no fixed payment numbers. *See* [11.1], *supra*. In the combination, Kobylkin describes that a “company name and/or *logo of the provider* of the instant disposable payment card can be *printed on the instant disposable payment card*.” Kobylkin, [0018]. Kobylkin further describes that “*the user's name* can be put on the instant disposable payment card.” *Id.* Kobylkin further describes that the “payment provider name or logo” can be “printed or otherwise provided on the instant disposable payment card.” *Id.*, [0029]; SAMSUNG-1003, ¶¶279-282.

(c) **Claim 15**

Element [15.0]

See [11.0], *supra*. SAMSUNG-1003, ¶283.

Element [15.1]

See [11.1], *supra*. SAMSUNG-1003, ¶284.

Element [15.2]

See [11.2], [11.5], *supra*. SAMSUNG-1003, ¶285.

Element [15.3]

See [11.6], *supra*. SAMSUNG-1003, ¶286.

Element [15.4]

See [11.2], *supra*. SAMSUNG-1003, ¶287.

Element [15.5]

In the combination, Smith’s mobile device includes a “***secure element chip***” (*i.e.*, a memory) that is “***configured to store***...mobile cloud account data” including a “***mobile cloud account number (MCA)***” (*i.e.*, payment card information). SAMSUNG-1006, [0003], [0012]. Smith further describes that the “processing device” of the mobile device “store[s] mobile cloud account data in the secure element,” thereby indicating that the secure element is accessible to the processor of the mobile device. *See, e.g., id.*, claim 22; dec; SAMSUNG-1003, ¶¶288-289.

Element [15.6]

See [11.7], *supra*. For example, 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 “card issuer provided payment card information” as recited in [15.6]. SAMSUNG-1003, ¶¶290-292.

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, ¶291.

Element [15.7]

As previously discussed (*see* [11.8], *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 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.” SAMSUNG-1007, 5:14-18; SAMSUNG-1003, ¶¶293-294. As previously discussed (*see* Section III.D.2-3, *supra*), a POSITA would have found it obvious to implement a cardholder authorization in Smith’s payment card device based on the teachings of Gomez.

Element [15.8]

There is no antecedent basis for or any description of “the payment information provided by the computing device” recited in this limitation. To the extent this term refers to the “limited-use payment information,” as previously discussed, Smith’s MCA and cryptogram are configured to be used in online

transactions (*see* [11.0], [11.10], *supra*) in place of a real card account number (RCA) (*i.e.*, a card issuers payment card information), and the cryptogram is further configured to be used in place of an ordinary issuer-provided verification value (*e.g.*, CVV1/CVV2/CVC1/CVC2 code) associated with a corresponding physical payment card. *See, e.g.*, SAMSUNG-1007, Abstract, 5:7-18, 13:1-4, 14:3-7, 21:5-19 (describing a system similar to Smith's in which a substitute account number (*e.g.*, Smith's MCA) and a cryptogram are used to "make purchases online"). SAMSUNG-1003, ¶¶295-297.

(d) Claim 16

Element [16.0]

See [12.0], *supra*. SAMSUNG-1003, ¶¶298-301.

(e) Claim 17

Element [17.0]

As previously discussed (*see* [11.8] and [15.7], *supra*), in the combination, Smith describes that its payment card device is configured to dynamically generate a limited-use payment information (the "payment cryptogram"). Gomez further discloses how a cryptogram for a transaction can be displayed on a device. SAMSUNG-1007, 13:1-4 ("cryptogram may be displayed"), 14:3-7. It would have been obvious to further modify the computing device in the combination so that the payment cryptogram would be displayable on a display of the computing device as taught in Gomez. SAMSUNG-1003, ¶303. A POSITA would have been

motivated to integrate Gomez's teaching for displaying a payment cryptogram in the computing device of the combination to facilitate online transactions, as expressly taught in Gomez. SAMSUNG-1007, 13:1-4, 14:1-7. 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. SAMSUNG-1003, ¶¶302-305. 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.*

(f) **Claim 18**

Element [18.0]

As previously discussed, in the combination, Smith describes a “***mobile cloud account number (MCA)***” (*i.e.*, a static limited-use card account number) “which may be associated with a real card account number (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.” SAMSUNG-1006, [0034]. Smith describes that the “generated MCA may include ***an expiration date***,” thereby indicating that the MCA is limited-use (*i.e.*, that it can only be used prior to the expiration date).

SAMSUNG-1006, [0086]; SAMSUNG-1003, ¶¶306-308. Also, as previously discussed (*see* [11.8], *supra*), Smith describes that its “payment cryptogram,” which is limited-use, “may be...a ***dynamic card validation code***” (*i.e.*, a limited-use card security code). SAMSUNG-1006, [0103].

Element [18.1]

See [11.9], *supra*. SAMSUNG-1003, ¶¶309-311.

(g) Claim 20

Element [20.0]

As previously discussed (*see* [15.7], *supra*), in the combination, 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.” SAMSUNG-1007, 5:14-18; SAMSUNG-1003, ¶¶312-314. Gomez further teaches that the “credential may be presented by a card user ***by swiping a fingerprint across a fingerprint sensor included within the card.***” SAMSUNG-1007, 7:11-13. As previously discussed (*see* Section III.B.3-4, *supra*), a POSITA would have found it obvious to implement a cardholder authorization in Smith’s payment card device based on the teachings of Gomez.

Element [20.1]

In the combination, Smith describes that the payment card device is operable to “display the mobile cloud account for the MCA to the user 302 in the form of ***an***

image of a payment card with first twelve digits of the MCA obscured (e.g., replaced by asterisks) and the last four digits displayed.” SAMSUNG-1006, [0083].

In addition, as previously discussed (*see* [15.7], *supra*), in the combination, 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-1007, 5:14-18; SAMSUNG-1003, ¶¶315-318. As previously discussed (*see* Section III.B.3-4, *supra*), a POSITA would have found it obvious to implement a cardholder authorization in Smith’s payment device based on the teachings of Gomez.

E. [GROUND 2B]: Claims 13 and 19 are obvious over Smith, Kobylkin, Gomez, and Varadarajan

1. Overview of Varadarajan

Varadarajan discloses techniques for “generating a dynamic card value (DCV) from a mobile user device for use in a transaction between a user cardholder and a transaction provider.” SAMSUNG-1015, Abstract; *see also id.*, [0002]. “The DCV may be configured for use as a card verification value (CVV), also known as a card security code” *Id.*, Abstract. “The DCV may be generated using a DCV generator which may include an algorithm and a DCV generation key.” *Id.* “The generated DCV is a dynamic card value, e.g., it is valid

or usable for a limited number of transactions or limited period of time.” *Id.*,

[0020]; *see also id.*, [0021], [0032], [0036]; SAMSUNG-1003, ¶¶101-102.

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

In the combination, the mobile device utilized in the Smith-Kobylkin-Gomez system from Ground 2A is further modified in view of Varadarajan to include a dynamic card value (“DCV”) generator. SAMSUNG-1015, [0025], [0020]-[0027], [0032]-[0036], Abstract. Based on Varadarajan, a user would invoke the DCV generator through a user interface on the device to request generation of a DCV value, e.g., a dynamic CVV. *Id.*, [0036]. The mobile device would be capable of displaying the DCV value on a display of the device. *Id.*, [0032], [0045]; SAMSUNG-1003, ¶¶319-321.

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

A POSITA would have found it obvious and would have been motivated to implement a DCV generator in the mobile device of the combination for multiple reasons. SAMSUNG-1003, ¶¶322-324. To start, Smith’s mobile device generates a “payment cryptogram” such as a “dynamic card validation code” for use in payment transactions, but discloses little detail about the specific algorithms or software used in generating the cryptogram. SAMSUNG-1006, [0011], [0067]. A POSITA would have turned to Varadarajan for additional detail on known

techniques for generating dynamic verification values like the payment cryptogram (e.g., dCVC) in Smith. SAMSUNG-1006, [0020]-[0021], [0011]-[0012].

In addition, or alternatively, it would have been obvious for the DCV generator to be installed on Smith's mobile device in the combination to facilitate payment transactions independently of the payment scheme disclosed in Smith. SAMSUNG-1003, ¶323. The user could then beneficially use the DCV generator for any of the myriad purposes described in Varadarajan, including to facilitate "card based transactions" and/or "card not present transactions" in circumstances where Smith's service is either not suitable or for use with cards that the user has not registered with Smith's service but for which a verification value is still needed. SAMSUNG-1015, [0022]-[0023], [0003]-[0006]. A POSITA would have understood that smartphones and other types of mobile devices of the types contemplated by Smith commonly allowed multiple applications to be installed before the Critical Date of the '820 patent, and consumers frequently utilized various applications on a mobile device to access different services independently of each other, thereby increasing the device's utility by increasing options and flexibility for the user to use the same device for various tasks. SAMSUNG-1006, [0033]; SAMSUNG-1015, [0026]; SAMSUNG-1003, ¶323. Moreover, a DCV generator like Varadarajan's would have been obvious and beneficial for use in the combination to increase security of payment transactions made using a dynamic

verification value in place of a static value by limiting opportunity for unauthorized actors to exploit a leaked value. SAMSUNG-1015, [0020]-[0021], [0022]-[0023]; SAMSUNG-1003, ¶323.

A POSITA would have been motivated to configure the mobile device to permit the user to provide an input through a user interface of the device to cause the DCV generator to generate a DCV. SAMSUNG-1015, [0036]. Enabling the DCV generator to respond to user input in this manner would have been beneficial to permit a new DCV value to be generated on demand when a user needs one for a particular transaction (e.g., an online transaction or to provide a DCV over the phone), and further would have allowed a user to input a PIN or other credential as a condition for generating the DCV in some examples to authenticate the user and increase security. SAMSUNG-1015, [0022]-[0023], [0032], [0036], Abstract; SAMSUNG-1003, ¶324. It further would have been obvious and a POSITA would have been motivated to present the DCV on a display of the device to permit a user to manually provide the DCV to a transaction interface (e.g., for online shopping or to be provided verbally over the phone). SAMSUNG-1015, [0032]; SAMSUNG-1003, ¶324; *see also id.*, SAMSUNG-1015, [0053]; SAMSUNG-1006, [0033]; SAMSUNG-1003, ¶324.

4. Analysis

(a) Claim 13

Element [13.0]

In the combination, Varadarajan describes a personal computing device (i.e., a mobile device) configured for presenting on the display a limited-use card security code (i.e., a DCV, “also known as a card security code (CSC)” such as a dynamic CVV). SAMSUNG-1015, [0032] (“DCV may be displayed”), [0045], [0020]-[0021], Abstract; *see also id.*, [0011]-[0015]. The DCV or card-security code “is valid or usable for a limited number of transactions or limited period of time,” and is used in place of card issuer payment information such as a static security code (e.g., static CVV). *Id.*, [0020], [0021]; SAMSUNG-1003, ¶¶325-327.

Element [13.1]

In the combination, Varadarajan discloses that the computing device is further configured to generate the limited-use DCV card security code responsive to an input request from a value user via a user interface of the device. SAMSUNG-1015, [0036], [0026]; SAMSUNG-1003, ¶¶328-329.

Element [13.2]

In the combination, Varadarajan discloses that the limited-use DCV card security code is generated using a “DCV key” stored on the personal computing device. SAMSUNG-1015, [0034]-[0035]. The DCV key itself can be generated based on various information such as a “card verification key (CVK) [applied] to the user’s account number and related account information, such as the card

expiration date and service code.” *Id.*, [0050]; SAMSUNG-1003, ¶¶330-332.

(b) Claim 19

Element [19.0]

See [13.0]-[13.2], *supra*. SAMSUNG-1003, ¶¶333-334.

Element [19.1]

See [13.0], *supra*. SAMSUNG-1003, ¶¶335-337.

F. [GROUND 2C]: Claim 14 is obvious over Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876

1. The combination of Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876

Mullen-876 discloses a payment device that generates a “dynamic expiration date” for use in payment transactions. SAMSUNG-1004, [0087]-[0088], [0092], [0105], [0107], FIG. 9. In the combination, the DCV generator on the mobile device of the Smith-Kobylkin-Gomez-Varadarajan combination from Ground 2B is further modified to generate and display a dynamic expiration date like that disclosed in Mullen-876. SAMSUNG-1015, [0032], [0045], [0020]-[0021], Abstract; *see also id.*, [0011]-[0015]; *supra*, Ground 2B at [13.0]; SAMSUNG-1003, ¶¶338-340.

2. Reasons to combine Smith, Kobylkin, Gomez, Varadarajan, and Mullen-876

A POSITA would have found it obvious and would have been motivated to configure the mobile device in the combination to generate a display a dynamic

expiration date having a limited-duration like that disclosed in Mullen-876 to improve payment transaction security. SAMSUNG-1003, ¶341. Similar to the various other forms of verification values disclosed in Mullen-876 and Varadarajan, a static expiration date could be exploited for a longer period of time or over more transactions than if the expiration date were dynamic and limited in use beyond just the time period indicated by the expiration date itself. SAMSUNG-1015, [0020]-[0021], [0022]-[0023]; SAMSUNG-1003, ¶341. It further would have been obvious and a POSITA would have been motivated to present the dynamic expiration date on a display of the device to permit a user to manually input the dynamic expiration date to a transaction interface (e.g., for online shopping or to be provided verbally over the phone). SAMSUNG-1015, [0032]; SAMSUNG-1003, ¶341.

3. Analysis

(a) Claim 14

Element [14.0]

In the combination, and for the reasons discussed, Smith-Kobylkin-Gomez-Varadarajan-Mullen-876 render obvious a personal computing device configured for presenting a DCV limited-use card account number (e.g., a dynamic PAN) and a limited-duration expiration date (e.g., a dynamic expiration date), for use in payments in place of a card issuer payment information. SAMSUNG-1004, [0087]-[0088], [0092], [0105], [0107], FIG. 9; SAMSUNG-1015, [0032], [0045],

[0020]-[0021], Abstract; *see also id.*, [0011]-[0015]; SAMSUNG-1003, ¶¶342-344.

Element [14.1]

See Ground 2B at [13.1], *supra*. SAMSUNG-1003, ¶¶345-346.

Element [14.2]

See Ground 2A at [15.7], *supra*. For example, in the combination, Gomez discloses that a limited-use number such as a payment cryptogram is generated “for each attempted transaction only after the cardholder successfully presents a credential, such as a fingerprint or a PIN number” to the payment device. SAMSUNG-1007, 5:14-18. Varadarajan also discloses that a PIN or other credential may be required to identify a valid device user before generating a DCV security code. SAMSUNG-1015, [0014], [0026], [0029], [0036], Abstract; SAMSUNG-1003, ¶¶347-349.

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 would be expected 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 June, 2024. The Board should not deny institution due to the close proximity of the FWD and disposition date.

SAMSUNG-1101, 3. With a gap of just over four months between the expected FWD and start of trial (*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).

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 IPR 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 ’820 patent that are the same as

those raised in this Petition.³ Thus, if IPR 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 about 3.5 months after service of Patent Owner’s preliminary infringement contentions and *identification of asserted claims* on September 8, 2022. SAMSUNG-1102; SAMSUNG-1105. In fact, Patent Owner asserted more than 100 claims against Samsung across five patents, and Petitioner has worked (and continues to work) diligently and efficiently to develop IPR grounds against each of the asserted claims. SAMSUNG-1105.

V. CONCLUSION AND FEES

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

³ Petitioner reserves all rights to pursue these invalidity grounds in the Related Litigation if IPR is not instituted.

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 ’820 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 has also filed IPR petitions against certain other patents that CardWare has asserted in the same civil action in E.D. Texas. These petitions have been assigned proceeding numbers IPR2023-00210, IPR2023-00211, IPR2023-00219, and IPR2023-00196.

Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the ’820 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: IPR39843-0144IP1@fr.com	Jeremy J. Monaldo, Reg. No. 58,680 Nicholas Stephens, Reg. No. 74,320 Daniel D. Smith, Reg. No. 71,278 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 IPR39843-0144IP1@fr.com

(referencing No. 39843-0144IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com, nstephens@fr.com and dsmith@fr.com).

Respectfully submitted,

Dated: December 23, 2022

/W. Karl Renner/

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

(Control No. IPR2023-00314)

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 *Inter Partes* Review totals 13,996 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated: December 23, 2022

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Nicholas Stephens, Reg. No. 74,320
Daniel D. Smith, Reg. No. 71,278
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 December 23, 2022, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via 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