

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

**SAMSUNG ELECTRONICS CO., LTD., and
SAMSUNG ELECTRONICS AMERICA, INC.,**

Petitioners,

v.

ICASHE, INC.,

Patent Owner.

Case IPR2025-00645
Patent No. 11,270,174

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	3
	A. Real Party-in-Interest	3
	B. Related Matters.....	3
	C. Lead and Back-Up Counsel.....	3
III.	PAYMENT OF FEES	4
IV.	REQUIREMENTS FOR INTER PARTES REVIEW	4
	A. Grounds for Standing	4
	B. Identification of Challenge.....	4
	1. The Specific Art on Which the Challenge Is Based	5
	2. Statutory Grounds on Which the Challenge Is Based	5
V.	'174 PATENT AND PROSECUTION HISTORY	6
	A. '174.....	6
	B. Prosecution History	9
VI.	§325(d) AND §314(a) DISCRETION DOES NOT APPLY	11
	A. §325(d)	11
	B. §314(a).....	14
VII.	LEVEL OF ORDINARY SKILL IN THE ART	19
VIII.	CLAIM CONSTRUCTION	19
IX.	GROUND OF UNPATENTABILITY.....	20
	A. Ground 1: Doughty in View of Abe (Claims 1-9)	20
	1. Overview of Doughty	20
	2. Overview of Abe.....	23
	3. Motivation to Apply Abe's Teachings to Doughty	24
	4. Claim Chart	28
	B. Ground 2: Doughty in View of Abe and Fox (Claims 1-9)	68
	C. Grounds 3-4: Grounds 1-2 in Further View of Dua (Claim 7)	72

D.	Grounds 5-6: Grounds 1-2 in Further View of Flitcroft (Claim 8).....	73
E.	Grounds 7-8: Grounds 1-2 in further view of Bursch (Claim 9)	76
X.	SECONDARY CONSIDERATIONS	78
XI.	CONCLUSION.....	79

EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001*	U.S. Patent No. 11,270,174 (“174”)
1002*	File History of U.S. Application No. 17/021,347 (“174FH”)
1003*	Declaration of Henry Dreifus in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent. No. 11,270,174 (“Dreifus”)
1004	U.S. Patent App. Pub. 2011/0240748 (“Doughty-CON”)
1005	U.S. Patent App. Pub. 2004/0133787 (“Doughty”)
1006-1007	<i>Reserved</i>
1008	Redline Between Doughty and Doughty-CON
1009	U.S. Patent No. 5,943,624 (“Fox”)
1010	U.S. Patent No. 7,917,444 (“Bursch”)
1011	U.S. Patent App. Pub. 2005/0086171 (“Abe”)
1012	U.S. Patent App. Pub. 2006/0165060 (“Dua”)
1013	U.S. Patent No. 6,636,833 (“Flitcroft”)
1014*	Plaintiff iCashe’s Infringement Contentions, Including Appx. H-1
1015-1027	<i>Reserved</i>
1028	U.S. Patent App. Pub. 2006/0017626 (“Kannan”)
1029	U.S. Patent No. 6,400,965 (“Phillips”)
1030	U.S. Patent No. 4,877,947 (“Mori”)
1031	<i>Reserved</i>
1032	U.S. Patent No. 5,466,919 (“Hovakimian”)

Exhibit No.	DESCRIPTION
1033-1035	<i>Reserved</i>
1036	U.S. Patent No. 6,670,796 (“Mori”)
1037-1040	<i>Reserved</i>
1041	U.S. Patent App. Pub. 2007/0236350 (“Nystrom”)
1042	Periodically, Merriam-Webster’s Collegiate Dictionary (11th ed., 2003)
1043	U.S. Patent App. Pub. 2006/0168418 (“Adusumilli”)
1044	U.S. Patent App. Pub. 2003/0004811 (“Omori”)
1045-1049	<i>Reserved</i>
1050	Docket Control Order, <i>iCashe, Inc. v. Samsung Electronics Co.</i> , No. 2:24-cv-00429-JRG (E.D. Tex.)
1051	Docket Control Order, <i>Valtrus Innovations Ltd. v. NTT Data Services, LLC</i> , No. 2:24-cv-00361, (E.D. Tex.)
1052	Docket Control Order, <i>Fleet Connect Solutions LLC v. The Kroger Co.</i> , No. 2:24-cv-00430 (E.D. Tex.)
1053	Docket Control Order, <i>C47 Technologies LLC v. TCL Technology Group Corporation f/k/a TCL Corporation</i> , No. 2:24-cv-00417 (E.D. Tex.)
1054	Docket Control Order, <i>SiOnyx, LLC v. Samsung Electronics, Co., Ltd.</i> , No. 2:24-cv-00408 (E.D. Tex.)
1055	Docket Control Order, <i>Stingray IP Solutions LLC v. Allegion Public Limited Company</i> , No. 2:24-cv-00396 (E.D. Tex.)
1056	Docket Control Order, <i>ElectraLED, Inc. v. Astera LED Technology GmbH</i> , No. 2:24-cv-00512 (E.D. Tex.)
1057	Docket Control Order, <i>Alto Dynamics, LLC v. Fresha.com SV Ltd.</i> , 2:24-cv-00468 (E.D. Tex.)
1058	Docket Control Order, <i>Cloud Byte LLC v. Dell Inc.</i> , No. 2:24-cv-00637 (E.D. Tex.)
1059	September 20, 2024 Production Letter in <i>iCashe, Inc. v. Samsung Electronics Co.</i> , No. 2:24-cv-00429-JRG (E.D. Tex.)

U.S. Patent No. 11,270,174
Petition for *Inter Partes* Review

Exhibit No.	DESCRIPTION
1060	December 12, 2024 Production Letter in <i>iCashe, Inc. v. Samsung Electronics Co.</i> , No. 2:24-cv-00429-JRG (E.D. Tex.)
1061*	Declaration of Cheryl Sloane in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 11,270,174
Petitioners have used the same exhibit number to refer to the same document across IPR2025-00642, -00643, -00643, -00644, and -00645, except for those exhibits designated by an *, which indicates that the exhibit is unique to each IPR proceeding.	

TABLE OF ABBREVIATIONS

Abbreviation	DESCRIPTION
'174	U.S. Patent No. 11,270,174 (“’174”) (Ex. 1001)
'174FH	File History of U.S. Application No. 17/021,347 (Ex. 1002)
Claims / Challenged Claims	Claims 1-9 of the '174
IPR	<i>Inter Partes</i> Review
Petitioners	Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America Inc.
PO	Patent Owner
POSITA	Person of Ordinary Skill in the Art
PTAB	Patent Trial and Appeal Board
USPTO	United States Patent and Trademark Office

LIST OF CHALLENGED CLAIMS

[1.pre] A mobile phone comprising:

[1.a] a memory to hold transaction data for use in a plurality of transactions;

[1.b] a current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;

[1.c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;

[1.d] a driver to excite the current carrying conductor; and

[1.e] a processor coupled to control the driver.

[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.

[3] The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.

[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.

[5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.

[6] The mobile phone of claim 1 wherein the driver comprises a current driver.

[7] The mobile phone of claim 1 wherein the network is one of a cellular network or

a wireless local area network.

[8] The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.

[9] The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.

Pursuant to §§311-319 and §42.1,¹ Samsung Electronics Co. Ltd. and Samsung Electronics America Inc. (“Petitioners”) respectfully petition for *inter partes* review of claims 1-9 (“Claims”) of U.S. Patent No. 11,270,174 (Ex. 1001, “’174”). There is a reasonable likelihood—and it is highly likely—that at least one challenged claim is unpatentable as explained herein. Petitioners request review of the Claims and judgment finding them unpatentable under §103.

I. INTRODUCTION

The ’174 is directed to a mobile phone that mimics a swipe of a magnetic card (e.g., credit card) by producing a time-varying magnetic field that represents transaction data (e.g., credit card data). ’174, 2:58-64, 3:42-48, 4:28-38, 5:38-53, 14:19-24, claims 1-2; Ex.1002 (’174FH), 1517-19. But these concepts were already known in the art as the USPTO already recognized during prosecution of the ’174. During its prosecution, the Examiner rejected the claims over Doughty-CON (Ex.1004), which is a continuation of and has substantially the same disclosures as

¹ Section cites are to 35 U.S.C. or 37 C.F.R. as context indicates. All emphasis/annotations added unless noted. Figure annotations herein generally quote the Claims for reference. Citations herein are exemplary and not meant to be limiting.

Doughty (Ex.1005)—a prior art reference relied upon in this Petition.² The claims were allowed only after the Applicant amended the independent claims to recite “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” Ex.1002, 1517-19, 1539, 1544-45. Ex.1003 (“Dreifus”) ¶40.

But the concept of a network interface to connect to a network to download transaction data was known. **Abe** discloses a system “to enable safer electronic commercial transactions,” operable for a “mobile telephone” to communicate with another device via a “network.” Abe, [0005], [0091], [0092], [0179], [0203], [0484]. **Abe** teaches that a “card identification number 351” is assigned to a “non-contact card” included in the mobile telephone, and is “provided via the network 10 by the authentication server 41” to enhance security. Abe, [0178]-[0179], [0308]. A POSITA would have been motivated to apply **Abe**’s teachings to **Doughty** to advantageously allow the device to download data used to perform electronic transactions as disclosed in Doughty. Dreifus ¶¶41-42.

Accordingly, Petitioners request that the Board institute trial and find the

² As discussed below in §V.2, the differences between **Doughty** and Doughty-CON are immaterial to the Examiner’s analysis during prosecution of the ’347-App. Dreifus ¶¶50-62.

Claims unpatentable.

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Party-in-Interest

Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. are the real parties-in-interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition.

B. Related Matters

The '174 is the subject of the following co-pending civil action:

iCashe, Inc. v. Samsung Elecs. Co., 2:24-cv-00429 (E.D. Tex) filed June 6, 2024 (“Texas Case”).

Petitioners have also filed petitions for IPR of the related U.S. Patents 8,403,219 (IPR2025-00642), 9,208,423 (IPR2025-00644) and 9,202,156 (IPR2025-00643).

C. Lead and Back-Up Counsel

Lead Counsel	Backup Counsel
James L. Davis, Jr. Reg. No. 57,325 ROPES & GRAY LLP 525 University Avenue, 8th Floor Palo Alto, CA 94301 Phone: +1-650-617-4000 Fax: +1-617-235-9492	Alexander E. Middleton Reg. No. 75,285 ROPES & GRAY LLP 1211 Avenue of the Americas New York, NY 10036-8704 Phone: +1-212-596-9000 Fax: +1-617-235-9492

james.l.davis@ropesgray.com Samsung-iCashe-IPR-Ropes@ropesgray.com Mailing address for all PTAB correspondence: ROPES & GRAY LLP IPRM—Floor 43 Prudential Tower 800 Boylston Street Boston, Massachusetts 02199-3600	alexander.middleton@ropesgray.com Frances Zhang Reg. No. 73,589 ROPES & GRAY LLP 2099 Pennsylvania Avenue, N.W. Washington, DC 20006-6807 Phone: +1-202-508-4600 Fax: +1-617-235-9492 frances.zhang@ropesgray.com
---	--

Petitioners consent to electronic service of documents to the email addresses of the counsel identified above.

III. PAYMENT OF FEES

The undersigned authorizes the Office to charge the fee required by §42.15(a) and any additional fees that might be due to Deposit Account No. 18-1945, under Order No. 110797-0057-656.

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Grounds for Standing

Pursuant to §42.104(a), Petitioners certify the '174 is available for IPR. Petitioners and any real parties-in-interest are not barred or estopped from requesting IPR challenging the Claims on the grounds identified herein.

B. Identification of Challenge

Pursuant to §§42.104(b) and (b)(1), Petitioners request IPR of the Claims and that the Board cancel the same as unpatentable.

1. The Specific Art on Which the Challenge Is Based

Petitioners rely upon the following art (Dreifus ¶¶69-72):

Name	Ex.	Publication	Filed	Published/ Issued	Prior art under at least
Doughty	1005	US2004/0133787	10/7/2003	7/8/2004	§§102(a)/ 102(e)
Abe	1011	US2005/0086171	7/15/2003	4/21/2005	§102(e)
Fox	1009	US5,943,624	7/15/1996	8/24/1999	§§102(a)/ 102(b)/ 102(e)
Dua	1012	US2006/0165060	1/21/2005	7/27/2006	§102(e)
Flitcroft	1013	US6,636,833	1/22/1999	10/21/2003	§§102(a)/ 102(b)/ 102(e)
Bursch	1010	US7,917,444	10/29/2002	3/29/2011	§102(e)

Each of the above references is prior art to the Claims based on the 2/22/2005 filing date of App. No. 11/063,291 listed in the '174's priority claim.

2. Statutory Grounds on Which the Challenge Is Based

Ground	Claim(s)	Basis	References
1	1-9	§103	Doughty in view of Abe
2			Doughty in view of Abe and Fox
3	7		Doughty in view of Abe and Dua
4			Doughty in view of Abe, Fox, and Dua
5	8		Doughty in view of Abe and Flitcroft

6			Doughty in view of Abe, Fox, and Flitcroft
7	9		Doughty in view of Abe and Bursch
8			Doughty in view of Abe, Fox, and Bursch

V. '174 PATENT AND PROSECUTION HISTORY

A. '174

The specification of the '174 discusses an “intelligent electronic device” (e.g., “mobile phone”) that internally communicates with an “electronic transaction card.” '174, Abstract, 2:58-3:10. The electronic transaction card “may be programmed to operate as a credit card” such that it “emit[s] one or more time-varying magnetic fields to emulate the swiping of a credit card.” '174, 5:38-44, 4:30-32, 11:47-59. “Electronic transaction card 104 may then be used with a magnetic stripe or smartcard based merchant point-of-sale terminal to effect a transaction.” '174, 4:32-35. According to the '174, “the term ‘transaction’ refers to any beneficial use of an electronic transaction card.” '174, 4:16-17. Dreifus ¶43.

As shown in Figure 22, the electronic transaction card includes **processing element 2020** coupled to “**magnetic/smartcard circuitry 2030**,” which “may include **circuits to produce time-varying magnetic fields** or **signals compatible with a smart card reader**.” '174, 11:67-12:2, 12:41-64, Figs. 20, 22. The electronic transaction device also includes “**volatile memory 2220**” storing “financial transaction data 2222.” '174, 12:47-52, Fig. 22. The **magnetic/smartcard circuitry**

2030 is coupled to the volatile memory 2220 via the processing element 2020 as shown in Fig. 22. Additionally, “magnetic field producing circuits 312 may include voltage drivers, [and] current drivers.” ’174, 6:64-67. “Intelligent electronic device 202 may include a mechanism to allow intelligent electronic device 202 to communicate with a wired or wireless network.” ’174, 5:8-10. For example, this mechanism “may include circuitry to communicate with a cellular phone network.” ’174, 5:11-12. The intelligent electronic device may also have “wired or wireless connectivity to a network other than a cellular network.” ’174, 5:22-23. Dreifus ¶44.

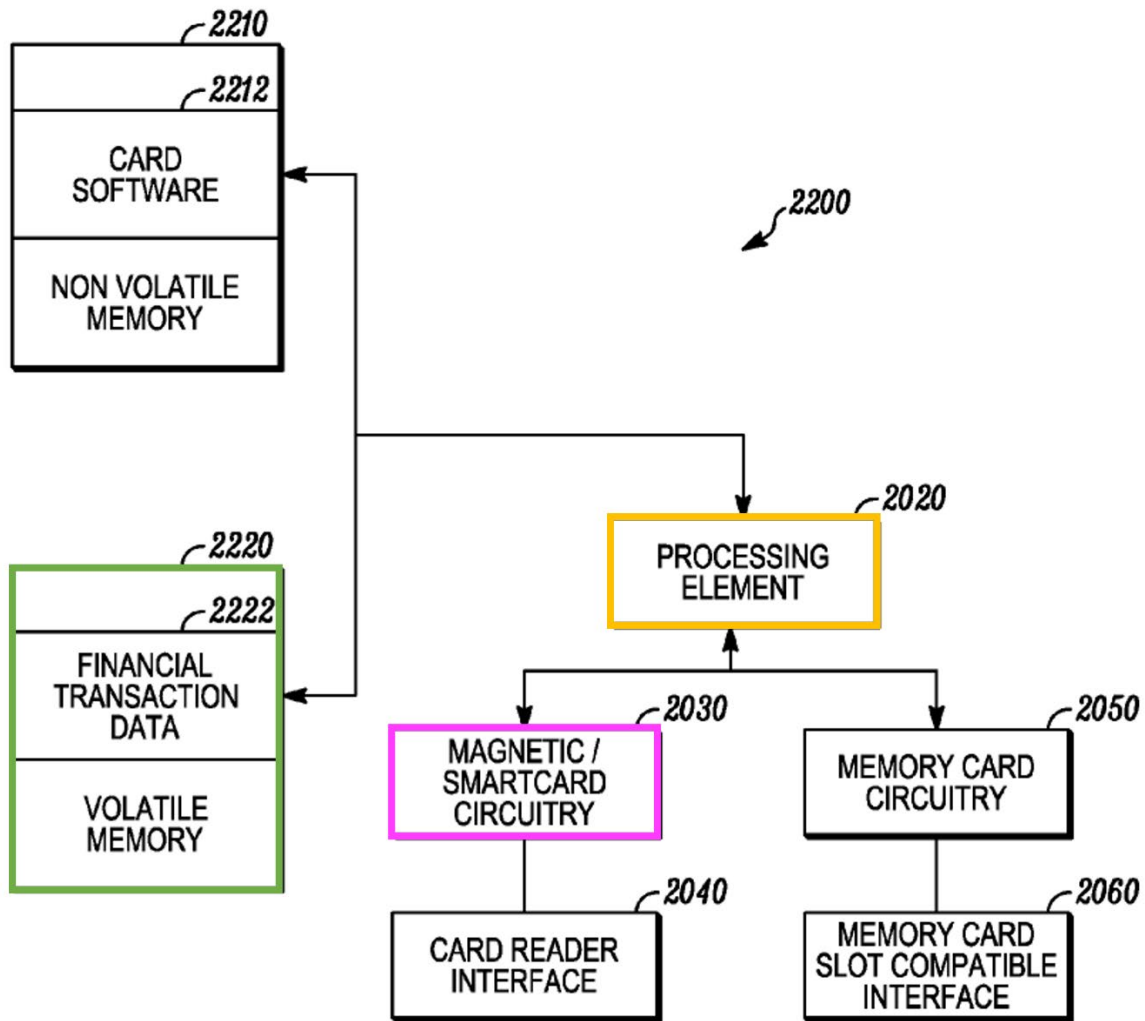


FIG. 22

The '174 discloses in another embodiment that a “processing device” “may read instructions from volatile memory 310 and/or nonvolatile memory 306 and perform actions in response thereto” and “execute program instructions that

influence communications between” the device and “a magnetic card reader.” ’174, 7:20-26. Dreifus ¶44.

B. Prosecution History

The ’174 issued from U.S. Pat. App. 17/021,347 (“’347 Application”), filed 09/15/2020. During prosecution of the ’174, the Examiner rejected claims 1-18 under §102 as being anticipated by Doughty-CON (U.S. Patent App. Pub. 2011/0240748). Ex. 1002, 1454. Dreifus ¶¶45-46.

While there are some minor differences in disclosure between Doughty-CON and **Doughty**, any substantive differences are not relevant to the material the Examiner identified as meeting limitations of the claims of the ’347-App. Ex.1008. Dreifus ¶¶47, 50-62.

The following chart summarizes the citations to Doughty-CON the Examiner found taught the ’174 pending Claims:

’174 (Pre-Amendment)	Doughty-CON (Disclosure Relied Upon By Examiner)³
[1.pre] A mobile phone comprising:	Doughty-CON [0046]
[1.a] a memory to hold transaction data for repeated use in a plurality of	Doughty-CON Fig. 3, 312 (“Memory”); [0009]

³ The same paragraphs numbers and figure numbers in **Doughty** have identical or substantively identical disclosures as the paragraphs and figures in Doughty-CON cited by the Examiner as identified in this chart. Dreifus ¶¶50-62

transactions;	
[1.b] current carrying conductor capable of producing a time-varying magnetic field that represents the transaction data in the plurality of transactions;	Doughty-CON Fig. 3, 308 (“Magnetic Field Generator”); [0051]
[1.d] a driver to excite the current carrying conductor;	Doughty-CON Fig. 5B, 554 (“Control Circuit”); [0051]
[1.e] a processor coupled to control the driver.	Doughty-CON Fig. 3, 314 (“Device Processor or Controller”); [0051]
[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	Doughty-CON [0008], [0095]-[0097]
[3] The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	Doughty-CON [0008], [0038]
[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	Doughty-CON [0008], [0038]
[5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	Doughty-CON [0051]
[6] The mobile phone of claim 1 wherein the driver comprises a current driver.	Doughty-CON [0051]

Ex.1002, 1454-1457. Dreifus ¶48.

In response, Applicant amended the independent claims to include the limitation “a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network.” Ex. 1002, 1517-19. Applicant also removed “repeated” from

“a memory to hold transaction data for repeated use in a plurality of transactions” in the independent claims. Ex. 1002, 1517-20. The claims were subsequently allowed on 11/10/2021. Ex. 1002, 1539, 1544-45. Dreifus ¶49.

VI. §325(d) AND §314(a) DISCRETION DOES NOT APPLY

A. §325(d)

Under the *Advanced Bionics* framework, there is no basis for discretionary denial under 35 U.S.C. § 325(d) as **the grounds raised by this Petition are not the same or substantially the same as the art and arguments raised during prosecution of the '174 patent.** *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Pap. 6, *8 (precedential) (establishing two-part framework for addressing 35 U.S.C. § 325(d)).

First, none of **Abe, Fox, Dua, Flitcroft, or Bursch** was identified in an IDS by the Applicant or considered by the Examiner. *See generally* '174FH.

Second, the Examiner never considered **Doughty** (or Doughty-CON) in combination with one or more of the other references employed in the grounds in this Petition, namely **Abe, Fox, Dua, Flitcroft, or Bursch**. The Examiner also never considered the testimony of Petitioners' expert Henry Dreifus (Ex.1003) regarding the scope and content of **Doughty, Abe, Fox, Dua, Flitcroft, or Bursch**. Dreifus ¶¶73-187.

Where a petition's grounds include new references that are non-cumulative of

the art previously evaluated by the Examiner during prosecution, those grounds are not the same or substantially the same art or arguments presented previously to the Office, even where the primary reference was considered by the Examiner. *Reflex USA LLC v. Longyear TM, Inc.*, IPR2023-00642 Pap. 11, *6-8 (declining to exercise §325(d) discretion where primary reference used in prosecution was combined with new reference); *see also Sony v. MZ Audio Scis., LLC*, IPR2022-01544, Pap. 12, *7 (§325(d) discretion improper where “Examiner did not consider the specific combination of references asserted”).

In *Reflex*, the Board determined that the first part of the *Advanced Bionics* framework was not satisfied where the Petition grounds combined a primary prior art reference previously presented to the Office with a new secondary reference that had not been identified in an IDS or considered by the Examiner. *Reflex* at *6, 8. The primary prior art reference, Beach-127, had been previously used to reject substantively similar claims during prosecution of grandparent and parent applications of the challenged patent. *Id.* at *6-7. Applicant overcame the rejections over Beach-127 in the grandparent and parent applications through the addition of a new limitation, which was also included in the challenged patent. To address this new limitation, the Petitioner combined Beach-127 with a new secondary reference, Wiese. *Id.* Though the Petition “relie[d] on Beach-127 essentially to teach the same

limitations that the Examiner previously found Beach-127 to teach or suggest,” the Board found that the addition of Wiese in the grounds made them not cumulative of the art previously presented to the Office, as Wiese “addresses the sole limitation in dispute.” *Id.*, *16. This is akin to the situation here: though **Doughty** here is being relied upon for essentially the same limitations that the Examiner had found Doughty-CON to teach, the grounds in this Petition combine the teachings of **Doughty** with the new and non-cumulative teachings of **Abe** to address the additional limitation added to overcome the rejections over the primary reference.

Furthermore, the disclosures considered by the Examiner are not substantially the same as any of the references relied upon in the Grounds of this Petition. For example, unlike the art cited during prosecution, **Abe** teaches a network interface for connecting the mobile phone to a network to download transaction data. Abe, [0179], [0187]. *See* §IX.A.4 Dreifus ¶¶78-159.

Even if the art or arguments were substantially the same, the Examiner erred in a manner material to the patentability of the Claims. Because the Examiner “did not expressly consider” nor issue any rejections based on the art relied on in this petition, it is difficult, if not impossible, to explain “why the Examiner allowed the claims” or “how the Examiner might have considered the arguments presented in the Petition.” *Bowtech, Inc. v. MCP IP, LLC*, IPR2019-00379, Pap. 14, *20 (declining

to exercise §325(d) discretion).

Indeed, the Examiner did not recognize any art teaching a network interface for downloading transaction data. To the extent art considered by the USPTO was substantially the same as the references identified in the Grounds, the Examiner erred by not rejecting the Claims for the reasons discussed in §IX. Dreifus ¶¶73-187.

The Board should not deny institution under § 325(d).

B. §314(a)

Co-pending district court litigation pending in the Eastern District of Texas also does not warrant the exercise of discretion under §314(a). *See Apple Inc. v. Fintiv, Inc.*, No. IPR2020-00019, Pap. 11 (designated precedential).

Factor 1 weighs in favor of institution. Petitioners intend to seek a stay of the district court litigation pending the outcome of this IPR, along with other IPRs related to the litigation dispute. At the time of institution, it is highly unlikely that the Court will have conducted a *Markman* hearing, which is currently scheduled for October 28, 2025. Ex. 1050, 3.

The Eastern District of Texas has routinely granted stays prior to claim construction, noting such cases have “not reached such an advanced stage that it would weigh against a stay.” *Broadphone LLC v. Samsung Elecs. Co.*, No. 2:23-CV-00001-JRG-RSP, 2024 WL 3524022, at *2-3 (E.D. Tex. July 24, 2024) (granting stay where “significant amount of discovery remains, the claim

construction hearing has not occurred, and trial is currently set for [over six months later]”). Even in cases that are far more advanced, the Eastern District of Texas has granted stays where an IPR has been instituted, recognizing “the PTAB’s insight and expertise ‘is likely to be of considerable assistance to the Court.’” *Onpoint Sys., LLC v. Protect Animals With Satellites, LLC*, No. 4:20-CV-657, 2022 WL 2704166, at *3-4 (E.D. Tex. July 12, 2022) (citation omitted) (granting stay even where “no dispute that this case is in an advanced stage”); *see also Cywee Grp. Ltd. v. Samsung Elecs. Co.*, No. 17-CV-00140, 2019 U.S. Dist. LEXIS 144149, at *19-22 (E.D. Tex. Feb. 14, 2019) (granting stay three months prior to scheduled trial date) (collecting cases where the court granted stays despite trial being four or fewer months away). Given the uncertainty of whether the district court will grant a stay in the litigation, this factor does not favor denial of institution.

To the extent the Board finds that **Factors 2 and 3** are neutral or at most weigh slightly against institution, they deserve little weight given Samsung’s diligence in preparing and filing this Petition. *Markman* briefing has not commenced; fact discovery is in its infancy (Ex. 1050, 4), with iCashe producing fewer than 250 pages beyond their patents, prosecution histories, and other public documents (Exs. 1059-60 (fewer than 11,200 pages total)); and no experts have prepared reports (Ex. 1050, 3). *See Apple v. Parus Holdings, Inc.*, No. IPR2020-00686, Pap. 9, 15–17 (aside

from initial invalidity contentions, finding “no other significant investment” where no dispositive motions, expert reports, or *Daubert* challenges occurred). Moreover, although trial is currently set for April 6, 2026, Petitioners expect the district court litigation will be delayed because twelve other active cases are also scheduled for trial on that same date and six of those were filed prior to this litigation. Exs. 1050-58; see *Boe Tech. Grp. Co. v. Optronix Scis. LLC*, No. IPR2024-01130, 2025 WL 305477, at *4 (P.T.A.B. Jan. 27, 2025) (*Fintiv* factor 2 “neutral or weigh[s] slightly in favor of not exercising discretion” where Judge Gilstrap “set 10 cases for jury selection on the same day”). The district court has also not issued any substantive orders, including any related to the validity of the ’174.

Petitioners’ diligence averts parallel, duplicative proceedings, and any unfair costs to Patent Owner. *Sotera Wireless, Inc. v. Masimo Corp.*, No. IPR2020-01019, Pap. 12, 16-17 (precedential as to § II.A); *Apple Inc. v. Maxell, Ltd.*, No. IPR2020-00204, Pap. 11, 16 (refusing to exercise discretionary denial even where trial would be complete nine months before FWD will issue, district court had already issued claim construction order, fact discovery had closed, and expert discovery was underway); *Lego Sys., Inc. v. Mq Gaming LLC*, No. IPR2020-01445, 2021 WL 606917, at *8 (P.T.A.B. Feb. 16, 2021) (granting institution where trial expected to occur “five months before a final written decision,” because outweighed by “low”

“investment by the court and parties in the [parallel case] on issues common to this proceeding,” Petitioner’s *Sotera* stipulation “that allays concerns about inefficient duplication of resources and the potential for inconsistent decisions,” and “the merits of the Petition are strong”); *CoolIT Sys., Inc., v. Asetek Danmark A/S*, No. IPR2021-01195, Pap. 10, 9-14 (instituting where district court trial was expected to occur five months before Board’s decision, and narrower Sand stipulation filed).

Importantly, fairness considerations weigh in favor of institution under *NHK*. *Fintiv*, Pap. 11, *11 (“[E]vidence...that the petitioner filed the petition expeditiously...weigh[] against exercising the authority to deny institution under *NHK*.”). iCashe has asserted multiple patents against Samsung. Samsung diligently investigated and assessed its options for challenging those patents (including the ’174) and had a right to do so before the statutory deadline for pursuing IPR expired. §315(b); *see also Lego*, 2021 WL 606917, at *5 (finding no delay supporting discretionary denial even where invalidity contentions had been served nearly a year prior, recognizing “preparing a petition for *inter partes* review requires substantial effort even after the references and basic theories have been identified”). This right should not be violated. iCashe’s selection of a venue with an expedited trial schedule should not be rewarded at the expense of Samsung’s rights to pursue review within one year of service of the complaint.

Factor 4 weighs strongly in favor of institution. Upon institution of this IPR proceeding, Petitioners stipulate that, they will not pursue in *iCashe, Inc. v. Samsung Elecs. Co.*, No. 2:24-cv-00429 (E.D. Tex. filed June 6, 2024), the grounds of invalidity asserted in the IPR, or any other ground that was raised or could have reasonably been raised in the IPR with respect to the Challenged Claims. *Sotera*, Pap. 12, *19 (finding “stipulation here mitigates any concerns of duplicative efforts...as well as concerns of potentially conflicting decisions” and “ensures that an *inter partes* review is a ‘true alternative’ to the district court proceeding”); *Lego*, 2021 WL 606917, at *6 (“[F]actor weighs strongly against discretionary denial” where “Petitioner has agreed to be bound by the same stipulation as in *Sotera*”).

Factor 5 is either neutral or weighs at most only slightly against institution. Petitioners and Patent Owner are the same parties in the district court litigation. While the overlapping parties may weigh slightly in favor of exercising discretion, institution and a public trial record of the important invalidity grounds in the Petition will reduce issues for the public, including all parties besides Samsung who may in the future be subject to litigation involving the ’174.

Factor 6 weighs strongly in favor of institution. The Petition is strong and presents compelling unpatentability arguments that were not previously considered during prosecution. The primary reference, **Doughty**, discloses all aspects of the

arrangement and components of the claimed mobile phone including hardware capable of producing a time-varying magnetic field to perform transactions other than downloading authentication information from an authentication server over a network. This additional limitation was well-known in the art and further described in **Abe**. See §IX. Dreifus ¶¶73-183. There is a significant public interest against “leaving bad patents enforceable,” *Thryv, Inc v. Click-ToCall Techs., LP*, 590 U.S. 45, 55 (2020). Accordingly, the Board should not exercise its discretion to deny institution. §314(a).

VII. LEVEL OF ORDINARY SKILL IN THE ART

On or before the claimed priority date of 2/22/2005, a person of ordinary skill in the art (“POSITA”) would have at least a Bachelor’s degree in electrical engineering, computer engineering, computer science, or the equivalent thereof, and approximately two years of professional experience in the field of electronic devices used for transactions. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Dreifus ¶¶63-66.

VIII. CLAIM CONSTRUCTION

Claim terms subject to IPR are to be construed according to the *Phillips* standard applied in district court. §42.100(b). Petitioners apply the plain and ordinary meanings of terms. Dreifus ¶¶67-68. Only terms necessary to resolve the

controversy must be construed.

IX. GROUNDS OF UNPATENTABILITY

This Petition is supported by the Declaration of Henry Dreifus, which describes the prior art's scope and content at the time of the '174. Dreifus ¶¶1-193.

Although the '174 purports to have invented an intelligent electronic device that can use an electronic transaction card to perform transactions, including by emulating the swipe of a magnetic card, such a system was already known. Dreifus ¶69. For example, **Doughty** describes a system for a user device having a magnetic field generator that can create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. In addition, **Abe** teaches using a network interface to download transaction data, such as authentication information, over a network to a mobile phone while performing a transaction. And **Fox** provides further detail regarding hardware for emitting a time-varying magnetic signal, including by using a driver to excite a current carrying conductor. And **Dua**, **Flitcroft**, and **Bursch** further teach features relating certain challenged dependent claims. As demonstrated below, the prior art renders the Claims unpatentable. Dreifus ¶¶70-183.

A. Ground 1: Doughty in View of Abe (Claims 1-9)

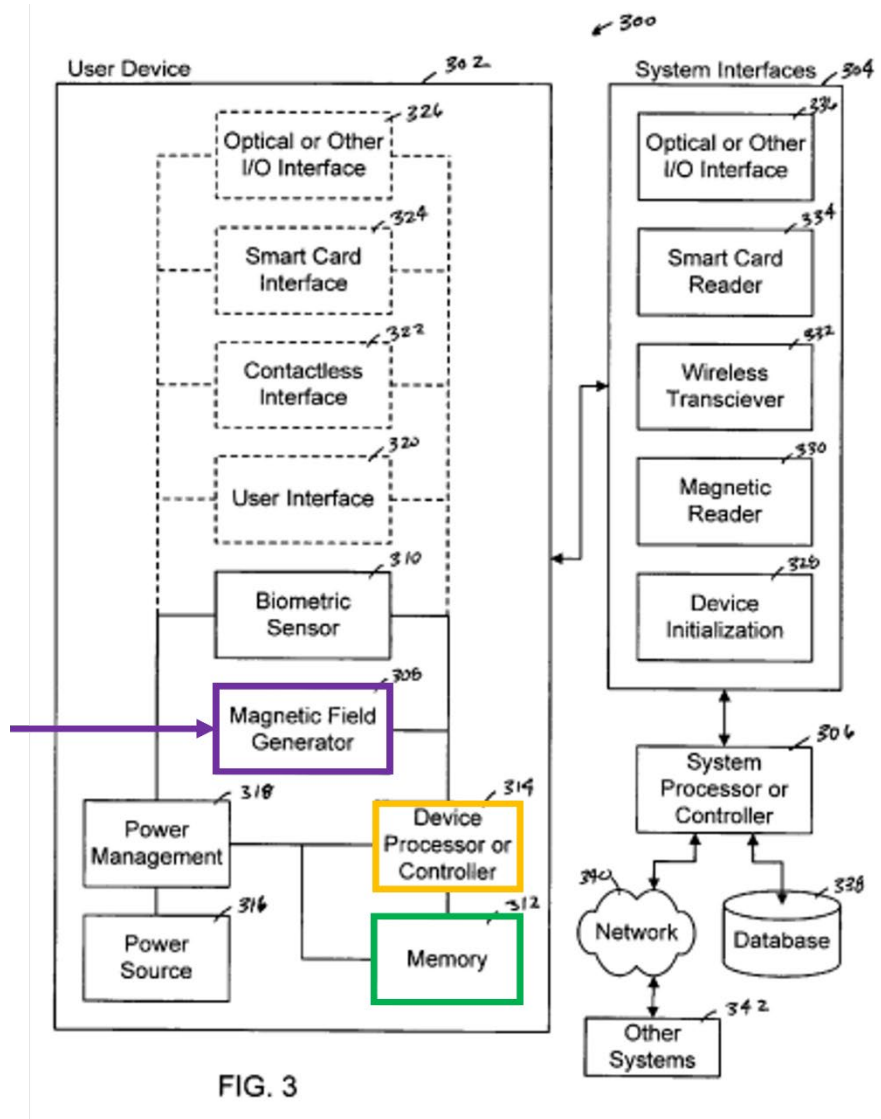
1. Overview of Doughty

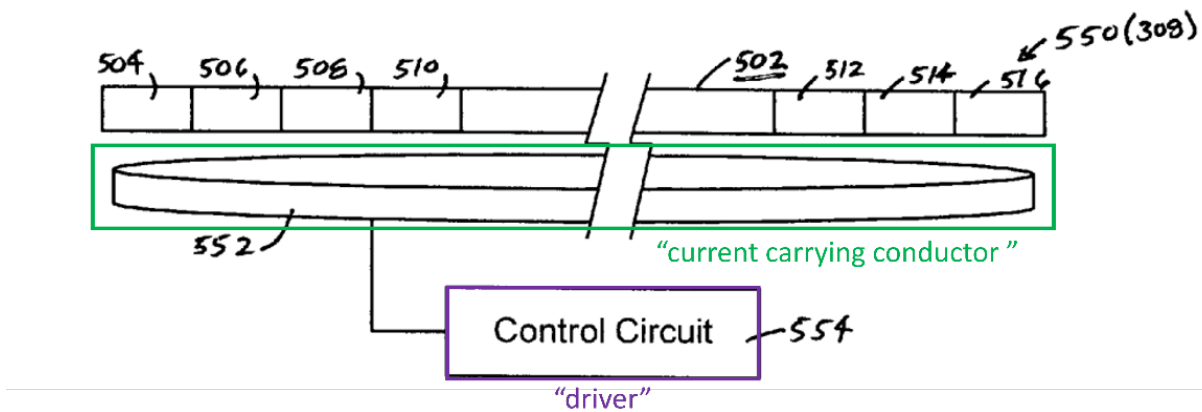
Doughty discloses a system in which a user device 302 includes components that can be mounted onto a substrate that is incorporated into a mobile device such as a “telecommunications device.” [0046]. User device 302 includes “**magnetic field generator 308**,” which can “create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” [0010]. Magnetic field generator 308 may have the form of a “programmable magnetic stripe 550” consisting of a “control circuit 554” and “a single inductive coil 552” such that the inductive coil 552 is “pulsed with varying currents and current directions” so as to emulate a time-varying magnetic field. [0051], Fig. 5B. A “**device processor or controller 314**” is coupled to magnetic field generator 308. [0040]. User device 302 also includes a “**memory 312**” for holding transaction data such as “binary data to enable a transaction.” [0040], [0041]. Dreifus ¶75.

User device 302 “can be used to enable any type of transaction” such as “an access transaction,” “a financial transaction,” or “a commercial transaction,” including a transaction with a “point-of-sale device.” [0054], [0098]. The disclosed commercial transactions may include credit card transactions. Doughty [0038]. Dreifus ¶76.

Figure 3 illustrates an exemplary embodiment of the user device 302 and Figure 5B illustrates the magnetic field generator, element 308 in Figure 3. Dreifus ¶77.

“circuitry to produce a time-varying magnetic field”



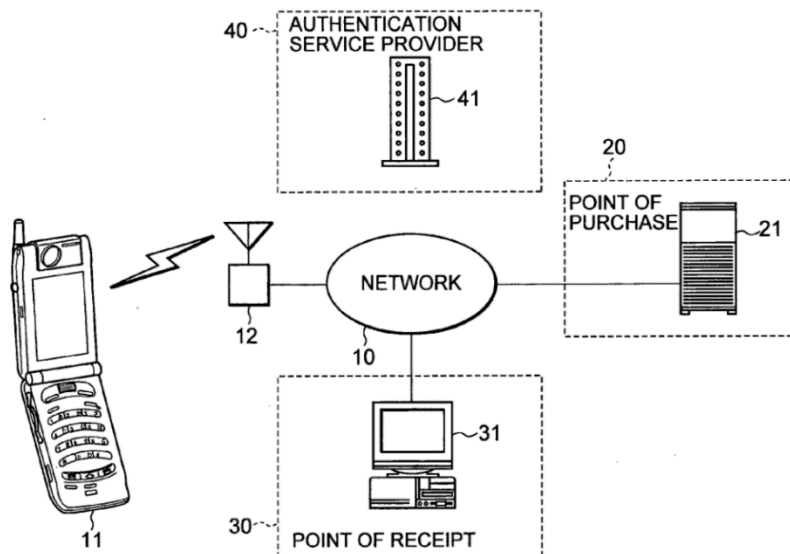


2. Overview of Abe

Abe discloses a system “to enable safer electronic commercial transactions to be carried out in a straightforward manner.” [0005]. **Abe** discloses a “mobile telephone 11” that communicates with another device via a “network 10.” [0091], [0092], [0179], [0203], [0484]. The mobile telephone receives transaction data from an “authentication server 41” via the network to authenticate a transaction. [0179], [0186], [0187], [0189], [0190], [0329]. For example, “temporary commercial transaction information rewriting key 362” and “card identification number 351” are provided to the mobile phone by the authentication server, which uses this information to perform a transaction. [0179], [0187], [0197], [0220], [0258], [0266], [0314], [0454]. “The card identification number 351...is a number for identifying the non-contact IC card 146” within the mobile telephone, and is provided “when the user of the mobile telephone 11 is registered as a purchaser of merchandise” with

an “authentication service provider 40.” [0178]-[0179]. The temporary commercial transaction information rewriting key is “a kind of one-time password” to perform a transaction that is deleted after use. [0187]. The authentication server “can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times.” [0187]. Dreifus ¶78.

FIG. 1



Abe, Fig. 1.

3. Motivation to Apply Abe’s Teachings to Doughty

Abe and **Doughty** are analogous art, in the same field as the ’174, which includes electronic devices for performing transactions, and are reasonably pertinent to purported problems addressed by the named inventors of the ’174 involving the use of electronic devices to securely perform transactions. ’174, 1:48-67, 5:29-37, 6:9-18, 12:41-64; Doughty [0002], [0003], [0004], [0007], [0008], [0038], [0040],

[0041], [0046]; Abe Abstract, [0001], [0002], [0003], [0004], [0005], [0006], [0179], [0183], [0509], [0510], [0511], [0512], [0513]; Dreifus ¶79.

A POSITA would have been motivated to apply **Abe**'s teachings of a mobile phone to **Doughty**'s telecommunications device. Dreifus ¶80. To the extent that it is argued that "telecommunications device" in **Doughty** refers to the more general class of devices communicating over a distance, instead of to a mobile phone specifically, a POSITA would have been motivated to look to a reference like **Abe**, which teaches examples of such telecommunications devices in which to implement functionality to perform commercial transactions, including a mobile telephone. Doughty, [0038], [0040]; Abe, [0091], [0092], [0179], [0203], [0484]. Dreifus ¶80. For example, a POSITA would have understood that integration of smartcard functionality into a mobile phone provides numerous advantages, including ease of use, enhanced security from theft or loss, and the ability to use the phone's display and input functionality to view and update/change information stored within the smartcard. Fox, 2:21-29. Dreifus ¶80. Moreover, a POSITA would have understood that implementing the functionality in a mobile phone would advantageously allow a user to perform commercial transactions with a device that a user would already be carrying around with them, including to locations where transactions would take place. Fox, 2:21-29. Dreifus ¶80. A POSITA would have found it straightforward

and advantageous to apply **Abe's** teachings to **Doughty** given **Doughty's** teaching that its system could be implemented in a variety of mobile devices, including a “telecommunications device.” **Doughty**, [0046]. Dreifus ¶80.

A POSITA would have also been motivated to apply **Abe's** teachings of downloading transaction data, such as a card identification number, from an authentication server over a network to **Doughty's** telecommunications device to advantageously improve the security of transactions, as desired by **Doughty**. Dreifus ¶81. For example, **Doughty** identifies the problem that “[t]he security of current magnetic stripe cards is suspect due to the ease of card theft and ‘skimming’ of card data for creating and using fake cards.” **Doughty**, [0003]. **Doughty** further explains that “the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value, and vendor-specific cards and/or devices.” **Doughty**, [0008]. Though **Doughty** discloses biometric authentication for authenticating the *user* performing a transaction (e.g., **Doughty** [0009]), it does not address how to protect against other security vulnerabilities contemplated by **Abe**, such as authenticating the *device* used to perform the transaction, and preventing the tampering of sensitive information used in the transaction. **Abe** [0179]; Dreifus ¶81. For example, **Abe** discloses that the authenticating server 41 supplies the mobile telephone used in the transaction

with a “card identification number 351” over the network 10 to ensure that the device performing the transaction is authentic as part of a user registration process. Abe, [0179], [0308]. Dreifus ¶81.

Additionally, a POSITA would have been motivated to apply **Abe’s** teachings of downloading temporary rewriting keys to **Doughty’s** telecommunications device to advantageously limit unauthorized tampering or use of sensitive information. Dreifus ¶82. For example, **Abe** discloses that “in order to prevent illegal duplication and falsification, it is not possible to make, edit or delete the temporary commercial transaction information without using the temporary commercial transaction information rewriting key 362.” Abe [0186]. Dreifus ¶82.

A POSITA would have found it straightforward to apply **Abe’s** teachings of downloading transaction data from an authentication server over a network to **Doughty’s** telecommunications device. Dreifus ¶83. For example, **Doughty** already teaches the use of binary data with various types of transaction data. Doughty, [0041]. A POSITA would have found it straightforward to download some of that data from a network as taught by **Abe**. Dreifus ¶83. Moreover, a POSITA would have found it straightforward, to include temporary transaction data and a card identification number as taught by **Abe** in the binary transaction data stored by

Doughty, as the temporary transaction data and card identification number would similarly be binary data in a form to be stored in memory. Dreifus ¶83.

Accordingly, a POSITA would have had a reasonable expectation of success applying **Abe**'s teachings to **Doughty**'s telecommunications device, and a POSITA would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶84.

4. Claim Chart

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
[1.pre] A mobile phone comprising:	To the extent that the preamble is limiting, Doughty discloses a mobile phone (<i>e.g.</i>, “personal communication device, such as...telecommunications device”). <u>E.g., Doughty</u> Doughty discloses a “personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager.” [0046]. The personal communication device includes a “user device 302” that is “disposed within or mounted on a substrate” that is “integrated into [the] personal communication device.” [0040], [0046], Fig. 3. A POSITA would have understood that Doughty's telecommunications device is a mobile phone.⁴ Dreifus ¶¶86-88. • Fig. 3:

⁴ Ex.1029, 1:14-16; Ex.1028, Abstract. Dreifus ¶88.

'174 Claim

Doughty (US2004/0133787) in view of Abe (US2005/0086171)

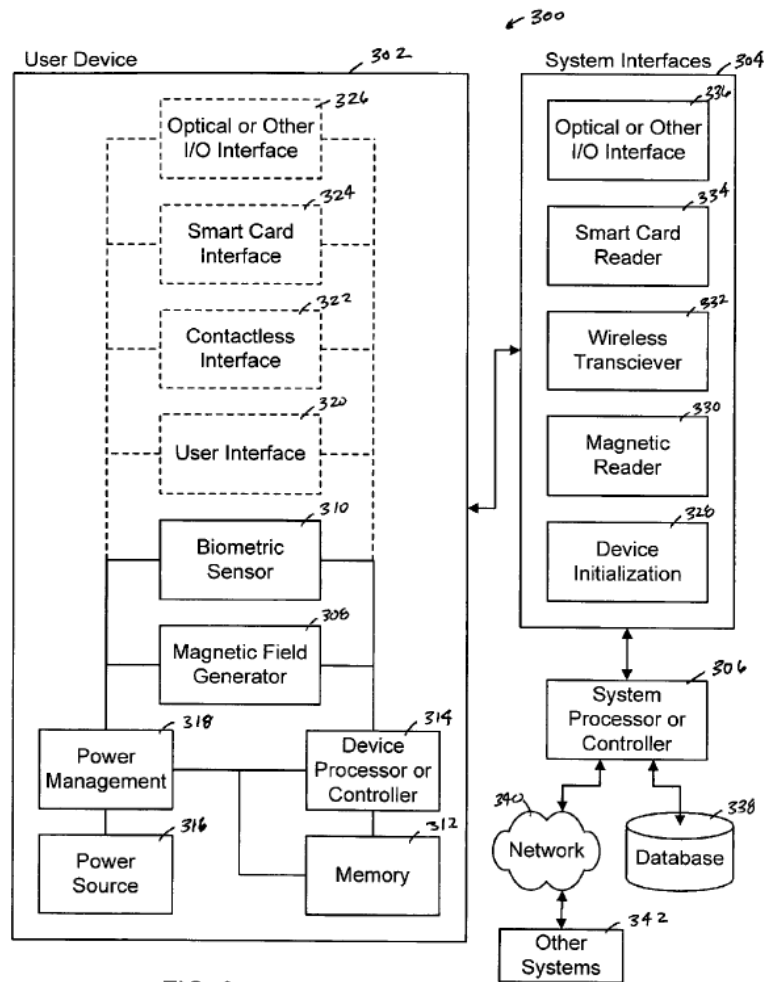


FIG. 3

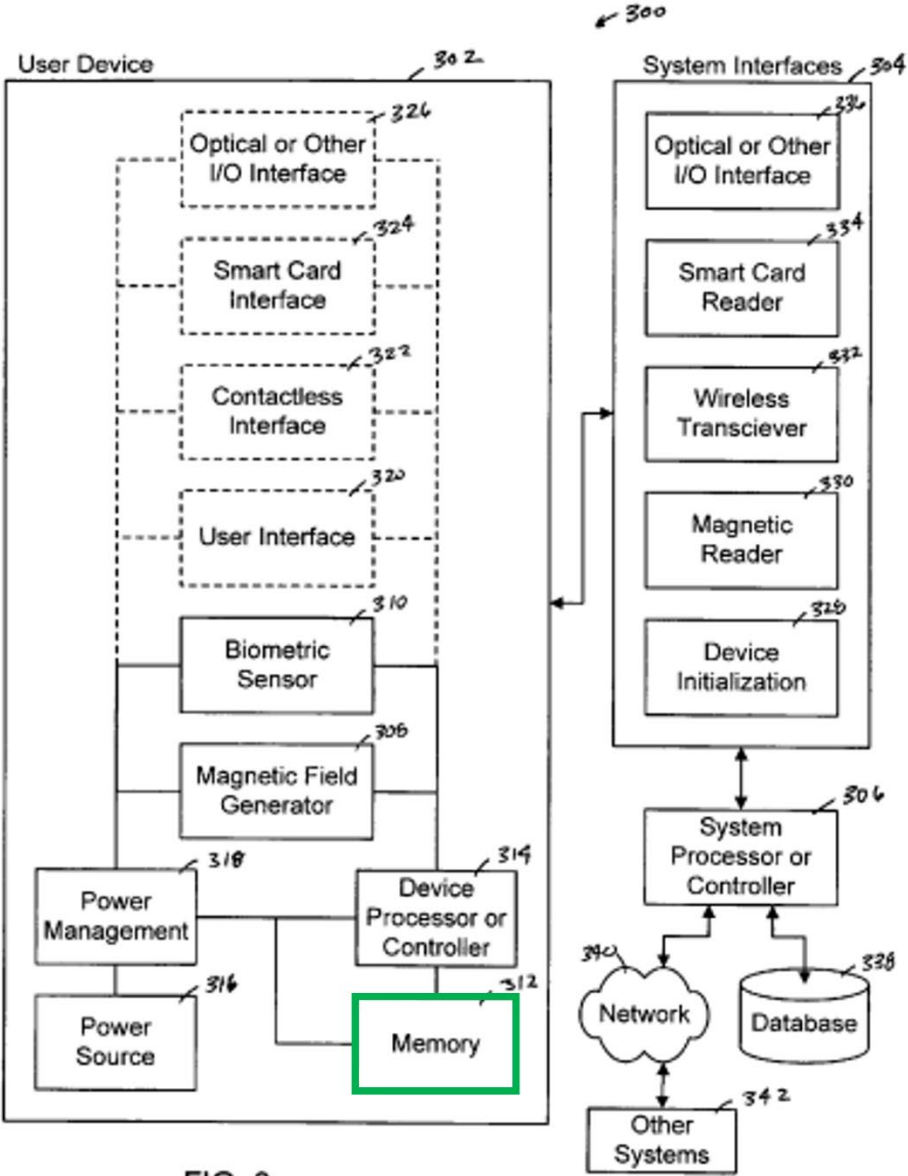
- [0040]:** “Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. *More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304.*”

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	[0046]: “The components of <i>the device 302</i> are typically disposed within or mounted on a substrate....In addition, <i>the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc....</i>” To the extent further disclosure is required, Abe discloses a mobile phone (e.g., “cellular mobile telephone 11”). <u>E.g., Abe</u> Abe discloses using a “cellular mobile telephone 11” to house hardware used to perform commercial transactions. Abe, [0092]-[0093], Fig. 1. Dreifus ¶¶89-90. As discussed in §IX.A.3, it would have been obvious to apply Abe’s teachings of a mobile phone to Doughty’s telecommunications device. Dreifus ¶91. Fig. 1 FIG. 1 <pre> graph LR 11[11: Mobile Phone] --- 12[12: Antenna] 12 --- 10((10: NETWORK)) 10 --- 40[40: AUTHENTICATION SERVICE PROVIDER] 40 --- 41[41: Tower] 10 --- 20[20: POINT OF PURCHASE] 20 --- 21[21: Server] 10 --- 30[30: POINT OF RECEIPT] 30 --- 31[31: Computer] </pre>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0092]: “In FIG. 1, <i>a mobile telephone 11 carries out wireless communication with and is connected to a nearest base station 12 so as to be connected to a network 10</i> to which the base station 12 is connected typified by, for example, the Internet, etc.” • [0093]: “<i>The mobile telephone 11 is operated by the user so as to carry out wireless communication with the nearest base station 12, access the point-of-purchase server 21 via the network 10, and carry out merchandise purchasing processing.</i>”
[1.a] a memory to hold transaction data for use in a plurality of transactions;	Doughty discloses a memory (<i>e.g.</i>, “memory 312”) to hold transaction data (<i>e.g.</i>, “binary data to enable a transaction”) for use in a plurality of transactions (<i>e.g.</i>, “transactions”). <u>E.g., Doughty</u> Doughty further discloses that the user device 302 includes “a memory 312” that stores data “for later transmission by the magnetic field generator 308.” [0040], [0041], Fig. 3. The time varying magnetic field transmitted by the magnetic field generator 308 includes “binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc.” [0040], [0041]. For example, the data stored in memory 312 can be read from a magnetic stripe of another device so that device 302 can replace the other device. [0040]. As such, a POSITA would have understood, or at minimum found it obvious, that the binary data to enable a transaction is stored in memory 312 to advantageously allow user device 302 to be used for transactions at a later time, after receiving the transaction data. Dreifus ¶¶92-94. Doughty further discloses that the transaction data stored in memory is used for a plurality of transactions. For example, Doughty discloses the “binary data” in the magnetic signal includes persistent data that would not change from one transaction to the next, such as the “user name,” “user number”

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	and “device expiration date.” [0041].⁵ Moreover, Doughty discloses device 302’s user name, user number and device expiration date are used across multiple transactions. For example, Fig. 3 represents a system for “enabling transactions” and Fig. 7 shows a flowchart for transactions in which after step 724 (“transaction complete”) the device returns to standby mode for initiating a new transaction. [0040], [0055], Fig. 7. As such, a POSITA would have understood, or at minimum found it obvious, that the memory is used to hold transaction data (such as “binary data to enable a transaction, such as a user name, user number, device expiration date”) corresponding to a plurality of transactions in order to enable transactions using the data. Dreifus ¶¶95-97. • Fig. 3:

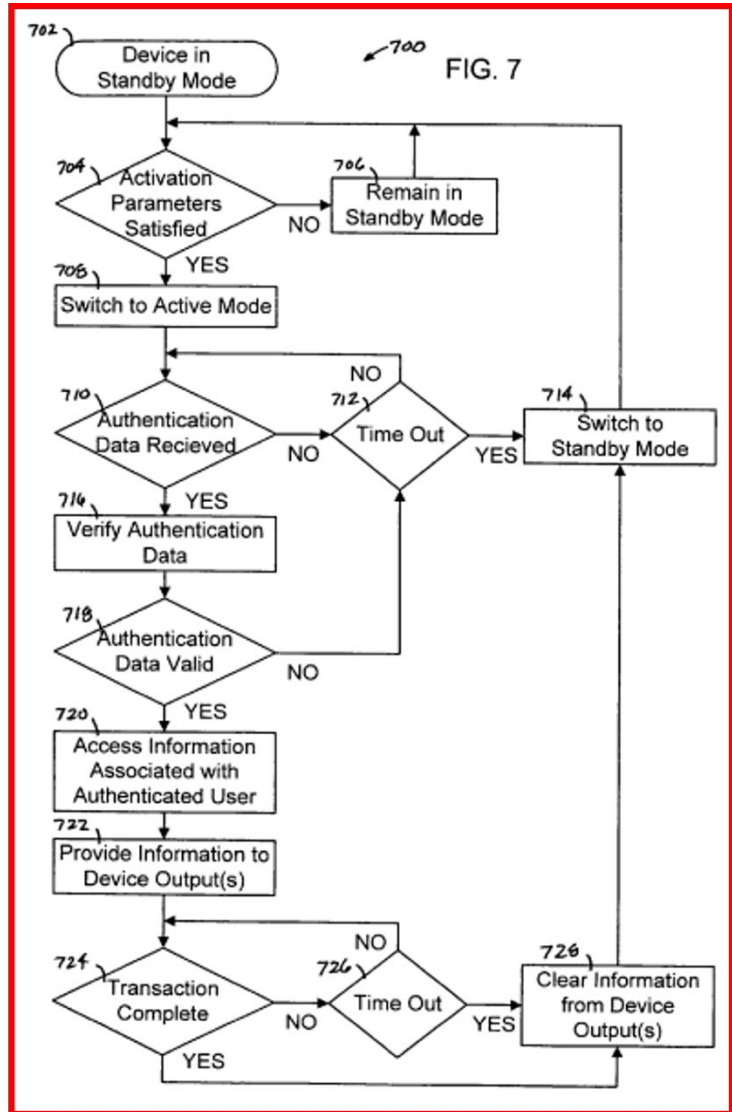
⁵ In this regard, **Doughty** discloses a card embodiment illustrated in Figure 4A in which “the cardholder’s name 410,” “card number 406” and “expiration date 408” are imprinted on the card, confirming the “user name,” “user number” and “device expiration date” are persistent across multiple transactions. Dreifus, ¶95.

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	 FIG. 3 • Fig. 7:

'174 Claim

Doughty (US2004/0133787) in view of Abe (US2005/0086171)

“transactions”

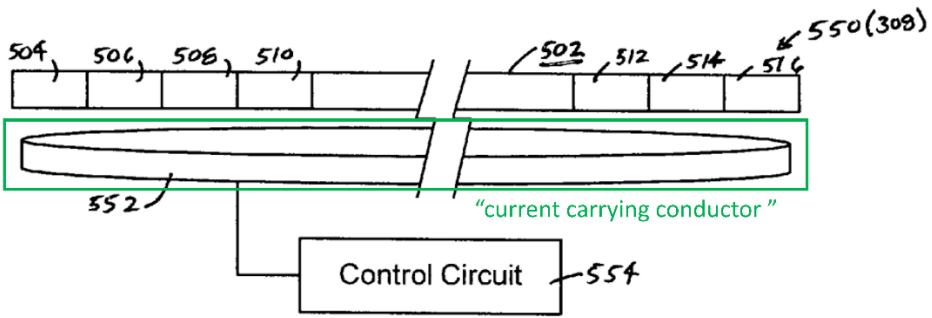


- [0040]: “Now referring to FIG. 3, *a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown*....Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, *a memory 312*, a device processor or controller 314 and a power source 316.”

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0041]: “In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc....Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. <i>The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication.</i>” • [0055]: “<i>Once the transaction is complete</i>, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and <i>the device waits for various activation parameters in block 704.</i>” • <i>See also</i> [0009]. To the extent further disclosure is required that the transaction data is used in a plurality of transactions, Abe discloses transaction data (e.g., “card identification number 351”) for use in a plurality of transactions (e.g., each “commercial transaction”). <u>E.g., Abe</u> Abe discloses that a “card identification number 351” is obtained as part of a user registration process to identify the “non-contact IC card.” [0179]. The card identification number 351 is provided to a “point-of-purchase server 31” during each “commercial transaction.” [0197]-[0198], [0245]-[0246]. Dreifus ¶¶98-99. As discussed in §IX.A.3, it would have been obvious to apply Abe’s teachings of downloading transaction data including a card identification number to Doughty’s telecommunications device. Dreifus ¶100.

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• Fig. 17: “transaction data for use in a plurality of transactions” FIG. 17 <pre> graph TD 1((1)) --> S71[REQUEST CARD IDENTIFICATION NUMBER INFORMATION S71] S71 --> S72{CARD IDENTIFICATION NUMBER INFORMATION ACQUIRED? S72} S72 -- NO --> S72 S72 -- YES --> S73[EXECUTE PURCHASING/CHARGE PROCESSING S73] S73 --> S74[PROVIDE PURCHASING INFORMATION S74] S74 --> S75{NOTIFICATION OF WRITING COMPLETION ACQUIRED? S75} S75 -- NO --> S75 S75 -- YES --> S76[PROVIDE NOTIFICATION OF PROCESSING COMPLETION S76] S76 --> S77{COMPLETE? S77} S77 -- YES --> END([END]) S77 -- NO --> 3((3)) 2((2)) --> S77 </pre> • [0179]: “<i>The card identification number 351 is a number assigned in advance to the non-contact IC card 146 and is a number for identifying the non-contact IC card 146. This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service.</i>”

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0197]: “The point-of-purchase server 21 that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then <i>makes a request to the mobile telephone 11 for the card identification number 351 allotted to the non-contact IC card 146</i> (arrow 376). The mobile telephone 11 then provides the card identification number 351 in response to this request.” • [0198]: “The point-of-purchase server 21 that has acquired the card identification number 351 then carries out processing relating to purchasing and charging, and sells the merchandise....” • [0245]: “To conform with this request, <i>in step S26</i> of FIG. 14, the main control unit 131 of <i>the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21.</i>” • [0246]: “<i>In step S72, the CPU 201 controls the communication unit 224 so as to determine whether or not card identification number information provided by the mobile telephone 11 has been acquired</i>, and waits until it is determined that acquisition has taken place.”
[1.b] a current carrying conductor capable of producing a time-varying magnetic field that	Doughty discloses a current carrying conductor (e.g., “inductive coil 552” of “programmable magnetic stripe 500”) capable of producing a time-varying magnetic field (e.g., “creat[ing] a time-varying magnetic signal”) that represents the transaction data (e.g., represents “binary data to enable a transaction”) in the plurality of transactions (e.g., “transactions”). <u>E.g., Doughty</u>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
represents the transaction data in the plurality of transactions;	See [1.a]. Doughty further discloses that “magnetic field generator 308” comprises “programmable magnetic stripe 550” including “inductive coil 552.” [0051], Fig. 5B. Each time the device is used, “magnetic field generator 308” creates a time-varying magnetic field that “includes binary data to enable a transaction.” [0041]. As discussed in [1.a], the binary data for enabling transactions would be used for each of a plurality of transactions. See [1.a]. Inductive coil 552 is a current carrying conductor that is “electrically connected” to the control circuit and is pulsed with “varying currents and current directions” to emulate a time-varying magnetic field. [0051]. Dreifus ¶¶101-104. Fig. 5B:  The diagram illustrates a magnetic field generator 308, which is a programmable magnetic stripe 550. The stripe is divided into seven segments, labeled 504, 506, 508, 510, 512, 514, and 516. Below the stripe, an inductive coil 552 is shown, which is a current carrying conductor. This coil is electrically connected to a control circuit 554. The entire assembly is labeled 550(308). [0041]: <i>“The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B)....In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc....”</i>

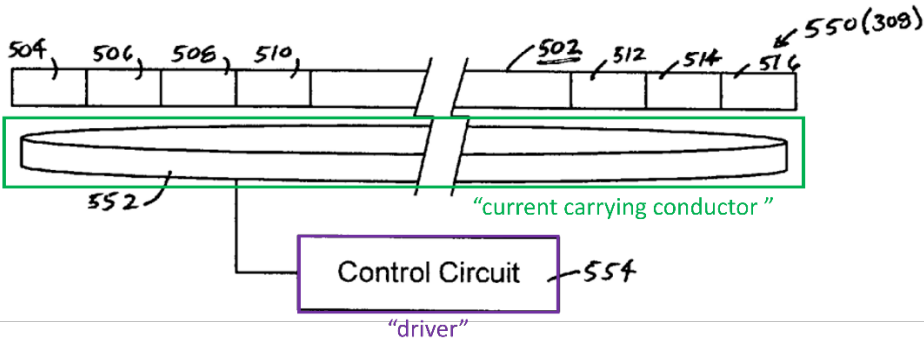
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0051]: <i>“Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554....The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader....In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502.”</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
[1.c] a network interface for connecting the mobile phone to a network, wherein one or more parts of the transaction data are downloadable to the mobile phone via the network;	Doughty discloses the mobile phone (<i>e.g.</i>, “telecommunications device”; <i>see</i> [1.pre]) and the transaction data (<i>e.g.</i>, “binary data to enable a transaction”; <i>see</i> [1.a]). <i>See</i> [1.pre]-[1.a]. Dreifus ¶¶105-107. Abe discloses a network interface (<i>e.g.</i>, antenna illustrated in Figure 1) for connecting the mobile phone (<i>e.g.</i>, “mobile telephone 11”) to a network (<i>e.g.</i>, “network 10”) wherein one or more parts (<i>e.g.</i>, “temporary commercial transaction information rewriting key 362” and/or “card identification number 351”) of transaction data (<i>e.g.</i>, transaction data received from “authentication server 41”) are downloadable to the mobile phone via the network (<i>e.g.</i>, “supplied”/ “provided” by the “authentication server 41” to the “mobile telephone 11” via “network 10”). <u>E.g., Abe</u> <i>See</i> [1.a]. Abe discloses that a “mobile telephone 11” communicates with “authentication server 41 via the network 10.” [0484], Fig. 1. For example, the mobile phone 11 includes an antenna (illustrated in Figure 1) that wirelessly connects with base station 12 in network 10, thereby providing an interface to network 10. [0092]. Dreifus ¶¶108-110. Abe further discloses that mobile telephone 11 receives various transaction information from authentication server 41, including “card identification number 351” and various “rewriting key[s]” that “prevent illegal duplication and falsification.” [0179], [0186]-[0187], [0189]-[0190], [0329], [0093], Fig. 24-26. For example, Abe discloses card identification number 351 is “provided via the network 10 by the authentication sever 41” to “mobile telephone 11.” [0179]. In addition, Abe discloses that its mobile telephone 11 is “provided” or “supplied a temporary commercial transaction information rewriting key 362” by the “authentication server 41” to authenticate a transaction performed by the mobile telephone

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	11. [0187]-[0188], [0329], Fig. 24-26. The information is provided by “authentication server 41” to “mobile telephone 11” through “network 10.” [0179], [0187]. Dreifus ¶111. As discussed in §IX.A.3, a POSITA would have been motivated to apply Abe’s teachings of downloading transaction data from an authentication server over a network to Doughty’s telecommunications device such that the downloaded transaction data is stored in the memory. Dreifus ¶¶112. Fig. 1: FIG. 1 <pre> graph LR 11[Mobile Telephone 11] --- 12[Antenna 12] 12 --- 10((Network 10)) 10 --- 40[Authentication Service Provider 40] 10 --- 20[Point of Purchase 20] 10 --- 30[Point of Receipt 30] 40 --- 41[Authentication Server 41] 20 --- 21[Device 21] 30 --- 31[Computer 31] </pre> [0093]: “<i>The mobile telephone 11 is operated by the user so as to access the authentication server 41 of the authentication service provider 40, trustworthiness of the point-of-purchase 20 is acquired, and this is provided to</i>

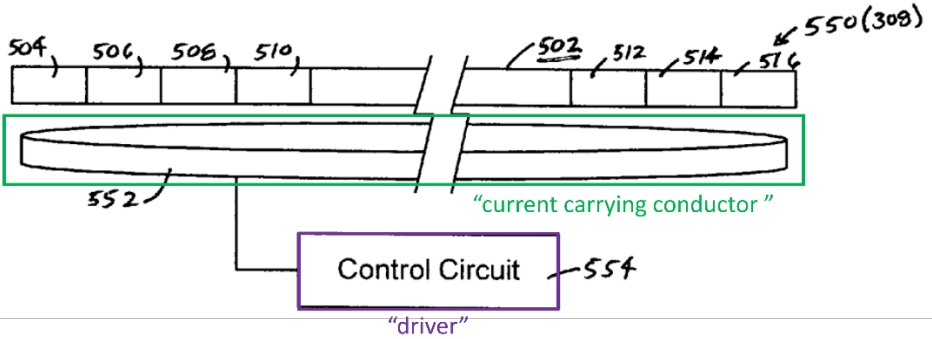
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	the user to enable a determination to be made as to whether or not to purchase the merchandise (product).” • [0179]: <i>“This card identification number 351 is provided by the authentication service provider 40 when the user of the mobile telephone 11 is registered as a purchaser of merchandise with this service. During this time, the card identification number 351 may be provided via the network 10 by the authentication server 41 or may be provided by the authentication service provider 40 using a separate method.”</i> • [0185]: <i>“The point-of-receipt server 31 shown in FIG. 11C stores the purchasing information rewriting key 361 described above and a temporary commercial transaction information rewriting key 362 constituting key information required in making, editing and deleting of temporary commercial transaction information described in the following in the storage unit 273.”</i> • [0186]: <i>“The temporary commercial transaction information rewriting keys 362 are distributed in advance by the authentication service provider 40 and is key information for making, editing and deleting etc. temporary commercial transaction information described in the following. Therefore, in order to prevent illegal duplication and falsification, it is not possible to make, edit or delete the temporary commercial transaction information without using the temporary commercial transaction information rewriting key 362.”</i> • [0187]: <i>“The temporary commercial transaction information rewriting key 362 is key information for making, editing and deleting etc. temporary commercial</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	transaction information. The temporary commercial transaction information rewriting key 362 is a kind of one-time password and is supplied to the mobile telephone 11 etc....The point of receipt server 31 and the authentication server 41 generating the temporary commercial transaction information rewriting key 362 can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times.” • [0329]: “As described in the following, the authentication server 41 that has acquired the notification of completion of writing provides a temporary commercial transaction information rewriting key 362 to the mobile telephone 11, and instructs the deletion of the temporary commercial transaction information 391 stored in the non-contact IC card 146.” • <i>See also</i> [0189], [0190], [0328], [0424].
[1.d] a driver to excite the current carrying conductor; and	Doughty discloses a driver (<i>e.g.</i>, “control circuit 554”) to excite the current carrying conductor (<i>e.g.</i>, “inductive coil 552”). <u>E.g., Doughty</u> <i>See</i> [1.b]. Doughty discloses that “inductive coil 552 is electrically connected to the control circuit 554,” and that “[b]y establishing the configuration in this manner, the inductive coil 442 can be pulsed with varying currents and current directions” so as to emulate a time-varying magnetic field. [0051], Fig. 5B. In order to effect the pulsing of the inductive coil with varying currents and current directions, a POSITA would have understood, or at minimum found it obvious, that the control circuit 554 is or at

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	least includes a driver to excite the inductive coil.⁶ Dreifus ¶¶113-116. Fig. 5B:  [0051]: “....<i>The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader....</i>”
[1.e] a processor coupled to	Doughty discloses a processor coupled to control the driver (e.g., “device processor or controller 314” “manage[s]” “control circuit 554”).

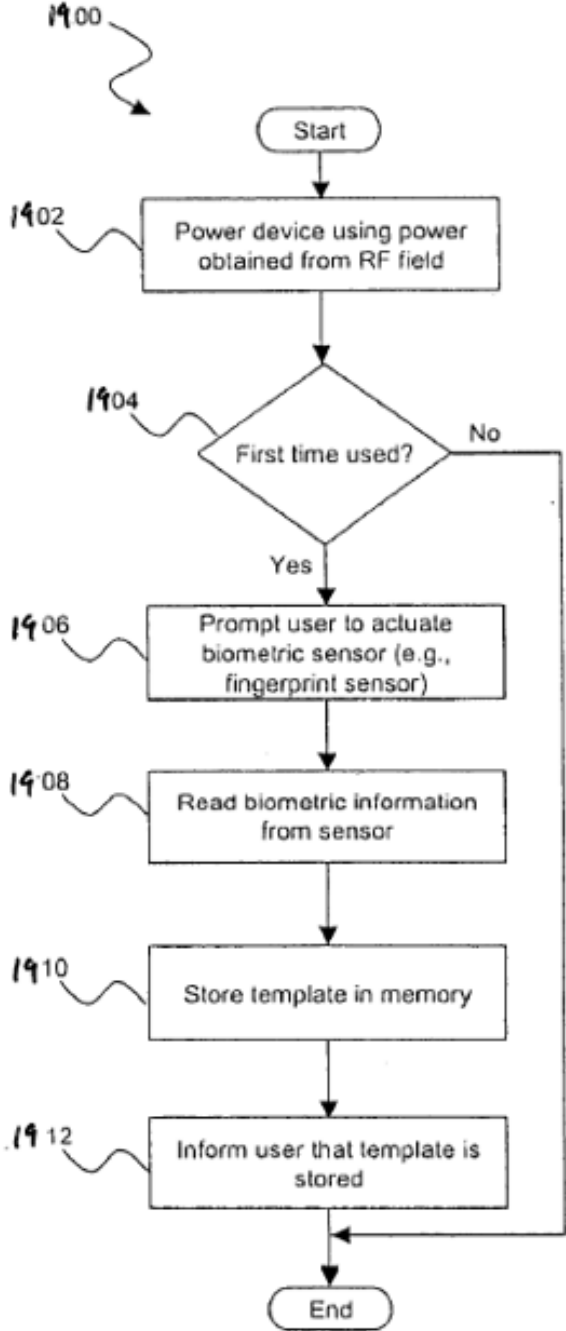
⁶ See, e.g., Ex.1036, 1:10-27 (disclosing driver circuit drives a current through an “inductive load”). Dreifus, ¶116.

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
control the driver.	<u>E.g., Doughty</u> <i>See</i> [1.d]. Doughty further discloses “device processor 314” is coupled to the driver (“control circuit 554,” <i>see</i> [1d]) because “control circuit 554” “may be integrated into the device processor 314,” but need not be integrated. [0051]. A POSITA would have understood, or at minimum found obvious, that control circuit 554 is coupled to device processor 314 when not integrated into the device processor 314. The processor/controller includes “logic” that “manages” the “programmable magnetic stripes 550 (308 FIG. 3),” which “includes...a control circuit 554” ([0039], [0051]). Thus, a POSITA would have understood, or at minimum found it obvious, that device processor 314 is coupled to the driver to control the driver of control circuit 554. Dreifus ¶¶117-120. • Fig. 3: “driver” (included in control circuit 554, which is included in programmable magnetic stripe 308) “coupled to” FIG. 3

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	Fig. 5B:  The diagram shows a magnetic stripe assembly 550 (308) with a current carrying conductor 552 and a control circuit 554 (driver). The conductor is connected to a series of magnetic tracks 504, 506, 508, 510, 502, 512, 514, and 516. [0039]: “The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and <i>programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device....</i>” [0051]: “...<i>The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554....The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3).</i>”
[2] The mobile phone of claim 1 wherein the time-varying magnetic field represents a point-of-sale transaction.	<i>See</i> [1]. Doughty discloses that the time-varying magnetic field (e.g., “time-varying magnetic signal”) represents a point-of-sale transaction (e.g., used for “any type of transaction” including “a financial transaction” or “a commercial transaction” with a “point of sale device”). <u>E.g., Doughty</u> <i>See</i> [1.b].

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	Doughty discloses the user device transmits a “time-varying magnetic signal” that carries “binary data to enable a transaction.” [0041]. Doughty further discloses that “the device can be used to enable any type of transaction.” [0054]. Doughty further discloses “the present invention provides a system, method, and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers,” and specifically “a secure and flexible system for security and/or commercial transactions using credit...cards.” [0038]. As such, a POSITA would have understood, or at minimum found obvious, that the time-varying magnetic signal represents a point-of-sale transaction. Dreifus ¶¶121-124. In addition, Doughty further discloses that Figures 19 and 20 provide “methods 1900 and 2000” for “using the present disclosure in a financial transaction environment.” [0095]. In describing this method, Doughty discusses specifically “device 800” as an exemplary device that can be used for the method, but a POSITA would have understood that device 302 is also part of the “present disclosure,” and methods 1900 and 2000 are thus equally applicable to device 302. [0054], [0095]-[0097], [0101]. Doughty discloses that, in method 1900, “retail purchases” are made by “hold[ing] the device 800 in the RF field generated by point-of-sale (‘POS’) device, which may be a kiosk, personal computer, cash register, or similar device” in order “[t]o register a selected fingerprint.” [0098], Fig. 19. Additionally, Doughty discloses that “device 800” is used to “authorize a payment transaction” by “hold[ing] the device 800 within a RF field generated by a RF reader connected to the POS device.” [0099], Fig. 20. Dreifus ¶125. To the extent it is argued that Doughty discloses method 1900 as a separate embodiment, not applicable to device 302, a POSITA would have found it obvious to use Doughty’s user device to perform point-of-sale transactions by communicating with a point-of-sale device to perform financial transactions using the time-varying magnetic signal. For example, a POSITA would have

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	understood that the use of device 302 for point-of-sale transactions would advantageously allow a user to conveniently purchase goods without the need to separately carry cards (e.g., credit cards) to perform those transactions. A POSITA would have had a reasonable expectation of success in using the device in this manner and known such an application (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶126. Fig. 7: “point-of-sale transaction” <pre> graph TD 702([702 Device in Standby Mode]) --> 704{704 Activation Parameters Satisfied} 704 -- NO --> 706[706 Remain in Standby Mode] 704 -- YES --> 706[706 Switch to Active Mode] 706 --> 710{710 Authentication Data Received} 710 -- YES --> 714[714 Verify Authentication Data] 710 -- NO --> 712{712 Time Out} 714 --> 718{718 Authentication Data Valid} 718 -- YES --> 720[720 Access Information Associated with Authenticated User] 718 -- NO --> 712 720 --> 722[722 Provide Information to Device Output(s)] 722 --> 724{724 Transaction Complete} 724 -- YES --> 726[726 Clear Information from Device Output(s)] 724 -- NO --> 726 726 --> 714[714 Switch to Standby Mode] 712 --> 714 714 --> 702 </pre>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• Fig. 19:  <pre data-bbox="500 373 1062 1696">graph TD; Start([Start]) --> 1402[Power device using power obtained from RF field]; 1402 --> 1404{First time used?}; 1404 -- No --> End([End]); 1404 -- Yes --> 1406[Prompt user to actuate biometric sensor (e.g., fingerprint sensor)]; 1406 --> 1408[Read biometric information from sensor]; 1408 --> 1410[Store template in memory]; 1410 --> 1412[Inform user that template is stored]; 1412 --> End;</pre> Fig. 19

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• Fig. 20: “point-of-sale transactions” <pre>graph TD; Start([Start]) --> 2002[Place device into RF field]; 2002 --> 2004[Actuate biometric sensor
(e.g., place finger on fingerprint sensor)]; 2004 --> 2006{Store transaction information?}; 2006 -- Yes --> 2008[Store transaction information]; 2006 -- No --> 2010[Remove device from RF field]; 2008 --> 2010; 2010 --> End([End]);</pre> Fig. 20 • [0038]: “The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges....As a result, <i>the present invention</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	<i>provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.</i> • [0041]: “The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal...<i>the magnetic signal includes binary data to enable a transaction</i>, such as a <i>user name, user number, device expiration date</i>, transaction approval/denial, etc.” • [0054]: “Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown....<i>The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction</i> or an identification transaction.” • [0095]: “Referring now to FIGS. 19 and 20, in another embodiment, <i>methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment</i>. The financial transaction environment includes making <i>retail purchases</i> in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment....” • [0098]: “Referring specifically to FIG. 19, before <i>the device 800 is usable in financial transactions</i>, it should be initialized by the buyer/owner with the registration of a selected fingerprint pattern into secured memory of the device 800. To register a selected fingerprint, <i>the device owner holds the device 800 in the RF field generated by a point of sale (“POS”) device, which may be a kiosk, personal computer, cash register, or similar device....</i>”

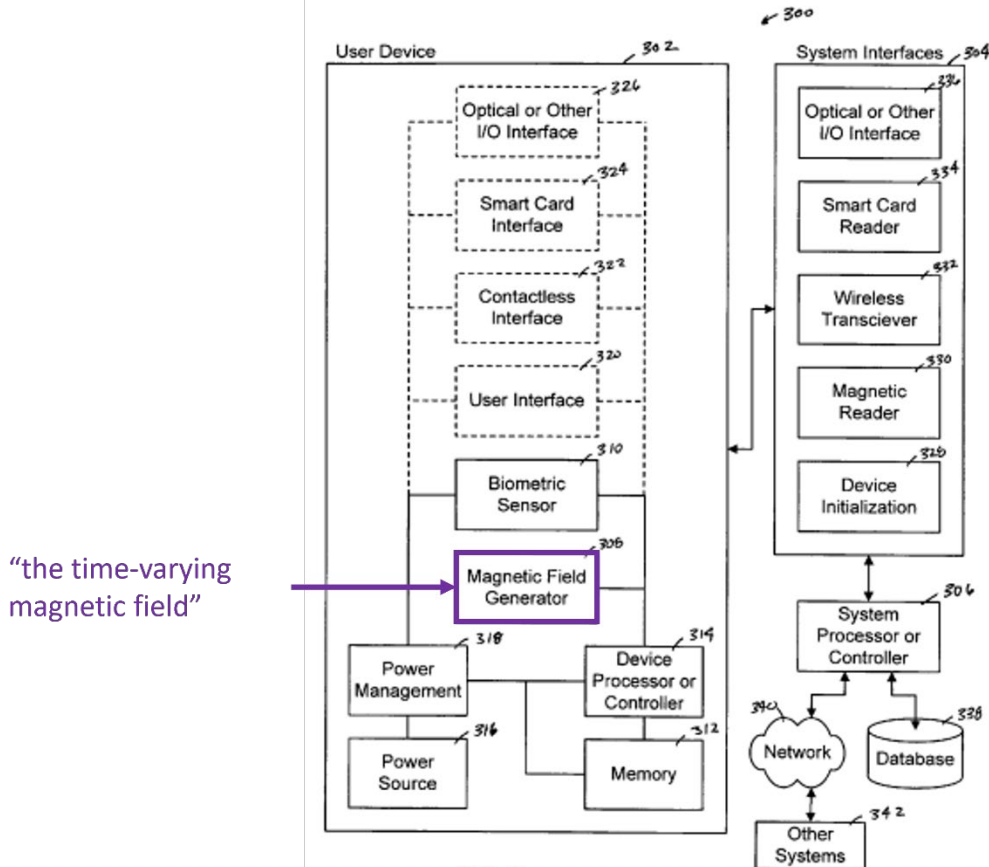
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0099]: “Referring specifically to FIG. 20, <i>to authorize a payment transaction</i> where invoice information is displayed by the POS device, <i>the user of the device 800 holds the device 800 within a RF field generated by a RF reader connected to the POS device</i> in step 2002....” • <i>See also</i> [0008], [0096]-[0097], [0101].
[3] The mobile phone of claim 1 wherein the time-varying magnetic field represents an access transaction.	<i>See</i> [1]. Doughty discloses that the time-varying magnetic field (<i>e.g.</i>, “time-varying magnetic signal”) represents an access transaction (<i>e.g.</i>, represents an “access transaction”). <u>E.g., Doughty</u> <i>See</i> [1.b]. Doughty further discloses the user device transmits a “time-varying magnetic signal” that carries “binary data to enable a transaction.” [0041]. Doughty further discloses that “the device can be used to enable any type of transaction, such as an access transaction.” [0054]. Dreifus ¶¶127-130. • [0008]: “...As a result, <i>the present invention provides a secure and flexible system for security and/or commercial transactions using access</i>, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.” • [0038]: “The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges....As a result, <i>the present invention provides a secure and flexible system for security and/or commercial transactions using access</i>, credit, debit,

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	identification, security, stored value and vendor-specific cards and/or devices.” • [0041]: “The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B)....<i>In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc....</i>” • [0054]: “The device can be used to enable <i>any type of transaction, such as an access transaction</i>, a control transaction, a financial transaction, a commercial transaction or an identification transaction.”
[4] The mobile phone of claim 1 wherein the time-varying magnetic field represents a credit card transaction.	See [1]. Doughty discloses that the time-varying magnetic field (<i>e.g.</i>, “time-varying magnetic signal”) represents a credit card transaction (<i>e.g.</i>, “commercial transactions using...credit...cards”). <u>E.g., Doughty</u> <i>See [1.b].</i> Doughty further discloses the user device transmits a “time-varying magnetic signal” that carries “binary data to enable a transaction.” [0041]. Doughty further discloses that “the device can be used to enable any type of transaction.” [0054]. Moreover, Doughty discloses that each of its interfaces—including magnetic field generator 308, which produces the time-varying magnetic field—is able to be used to perform such transactions. [0055]. Doughty further discloses that “the present invention provides a system, method, and apparatus for a practical and secure card or

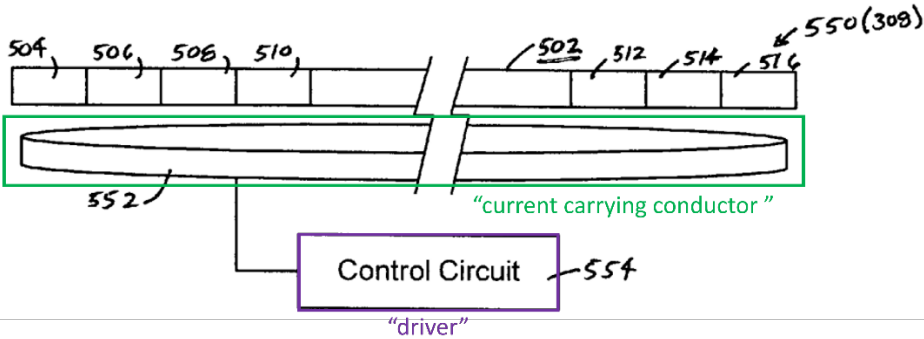
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers,” and specifically “a secure and flexible system for security and/or commercial transactions using credit...cards.” [0038]. Consistent with this, Doughty further discloses that the “magnetic field generator 308” is in the form of a “magnetic stripe” that transmits “a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” [0010], [0040], [0041], [0051], Fig. 3. A credit card has a magnetic stripe.⁷ As such, a POSITA would have understood, or at minimum found obvious, that the time-varying magnetic signal represents a credit card transaction. Dreifus ¶¶131-134. • [0008]: “...As a result, <i>the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.</i>” • [0038]: “The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges....<i>As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.</i>” • [0041]: “The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial

⁷ See, e.g., Ex. 1032, 2:16-17, 31-32. Dreifus, ¶134.

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B).... <i>In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc....</i> • [0054]: “The device can be used to enable <i>any type of transaction</i>, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.”
[5] The mobile phone of claim 1 wherein the time-varying magnetic field emulates a swipe of a magnetic card.	<i>See [1].</i> Doughty discloses the time-varying magnetic field (e.g., “time-varying magnetic signal”) emulates a swipe of a magnetic card (e.g., “emulating data obtained from swiping a magnetic stripe card”). <u>E.g., Doughty</u> <i>See [1.b].</i> Doughty further discloses that the “magnetic field generator 308” is in the form of a “magnetic stripe” that transmits “a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.” [0010], [0040], [0041], [0051], Fig. 3. Dreifus ¶¶135-138. • Fig. 3:

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	 "the time-varying magnetic field" FIG. 3 [0010]: "The present invention provides an apparatus or user device that includes a substrate, <i>a magnetic field generator disposed within the substrate</i> that is normally inactive...and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory.... The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or <i>create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader</i>. As a result, the magnetic field generator emulates a programmable magnetic stripe."

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0040]: “<i>Each user device 302 includes a magnetic field generator 308</i> that is normally inactive.... The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified.” • [0041]: “<i>The magnetic field generator 308 emulates a programmable magnetic stripe</i> by either creating a spatial magnetic signal or <i>a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.</i>” • [0051]: “The programmable magnetic stripe 550 (308 FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554....The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that <i>a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader.</i>.... By establishing the configuration in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. <i>This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card</i> with the desired information embedded in the individual data cells 504-516 of the stripe 502.”
[6] The mobile phone	<i>See [1].</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
of claim 1 wherein the driver comprises a current driver.	Doughty discloses that the driver comprises a current driver (e.g., driver that “pulses” the inductive coil with “varying currents and current directions”). <u>E.g., Doughty</u> See [1.d]. As discussed above for [1.d], Doughty discloses or renders obvious a driver (e.g., “control circuit 554”) to excite the current carrying conductor (e.g., “inductive coil 552”). See [1.d]. Moreover, Doughty discloses that “inductive coil 552” is “pulsed with varying currents and current directions” so as to emulate a time-varying magnetic field. [0051], Fig. 5B. Because the current is driven through the antenna, the driver disclosed or rendered obvious by Doughty is a current driver. Dreifus ¶¶139-142. Fig. 5B:  [0051]: “Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308 FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown....<i>The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	<i>in this manner, the inductive coil 552 can be pulsed with varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502."</i>
[7] The mobile phone of claim 1 wherein the network is one of a cellular network or a wireless local area network.	<i>See</i> [1]. Abe discloses the network (e.g., "network 10") is a cellular network (e.g., cellular network with "base station 12" over which "mobile telephone 11" communicates). <u>E.g., Abe</u> <i>See</i> [1.c]. As discussed in [1.c], Abe discloses that a "mobile telephone 11" communicates with "authentication server 41 via the network 10." [0484], Fig. 1. Moreover, Abe discloses that mobile telephone 11 communicates with the network 10 via a base station 12. [0092]. A base station is a network component commonly used in cellular networks for use by a mobile phone to communicate data.⁸ As

⁸ Ex.1028, [0008] (explaining that "wireless networks are increasingly being used for data communication...so that mobile-phone users can access Internet-based resources"), [0005] (explaining that mobile phones "communicat[e] with base stations"). Dreifus, ¶146

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	such, a POSITA would have understood, or at minimum found it obvious, that the mobile telephone 11 is communicating with the authentication service provider 41 over a cellular network or a wireless local area network. Dreifus ¶¶143-146. As discussed in §IX.A.3, a POSITA would have been motivated to apply Abe's teachings of downloading transaction data to Doughty's telecommunications device. Dreifus ¶¶147. Fig. 1: FIG. 1 <pre> graph LR 11 --- wireless 12 12 --- 10 10 --- 41 10 --- 21 10 --- 31 subgraph 40 [AUTHENTICATION SERVICE PROVIDER] 41 end subgraph 20 [POINT OF PURCHASE] 21 end subgraph 30 [POINT OF RECEIPT] 31 end </pre> [0092]: “In FIG. 1, a <i>mobile telephone 11</i> carries out <i>wireless communication with and is connected to a nearest base station 12</i> so as to be connected to a network 10 to

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	<i>which the base station 12 is connected typified by, for example, the Internet, etc....”</i>
[8] The mobile phone of claim 1 wherein downloaded transaction data is valid for a limited number of transactions and the one or more parts of the transaction data is downloaded periodically.	<i>See [1].</i> Abe discloses that downloaded transaction data (<i>e.g.</i>, “temporary commercial transaction information rewriting key 362”) is valid for a limited number of transactions (<i>e.g.</i>, “one-time”) and the one or more parts (<i>e.g.</i>, “temporary commercial transaction information rewriting key 362”) of the transaction data (<i>e.g.</i>, transaction data received from “authentication server 41”) is downloaded periodically (<i>e.g.</i>, supplied to the mobile telephone for each transaction). <u>E.g., Abe</u> <i>See [1.a], [1.c].</i> As discussed in [1.c], Abe discloses that its mobile telephone 11 downloads “temporary commercial transaction information rewriting key 362” from the “authentication server 41” to authenticate a transaction performed by the mobile telephone 11. <i>See [1.c].</i> Abe further discloses that “temporary commercial transaction rewriting key 362” is a “one-time password”⁹ that is “supplied to the mobile telephone 11” during the course of a transaction and therefore is downloaded transaction data. Figs. 24-26, [0187], [0329]. After temporary commercial transaction information is updated, the mobile phone deletes the temporary

⁹ A value used for a single transaction meets the claim language requiring a “limited number of transactions.” This is consistent with the ’174, which also discloses a single-use “single transaction account number” in which its card uses “a different number for each transaction.” ’174, 5:44-52. Dreifus ¶151.

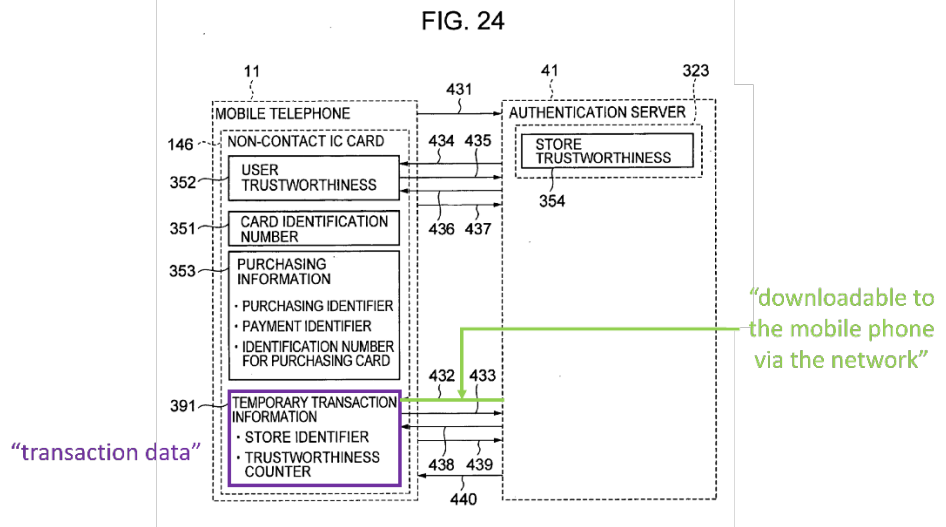
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	commercial transaction rewriting key 362. [0187], [0330]. The authentication server supplies new temporary commercial transaction rewriting keys “any number of times.” [0187]. Dreifus ¶¶148-151. To the extent it is argued that “limited number of transactions” requires multiple transactions, it would have also been obvious to use a password for some other limited number of times (e.g., two) such that it advantageously does not need to be downloaded as often. Dreifus ¶152. Because the temporary commercial transaction rewriting keys are downloaded “any number of times” for a given transaction ([0187]), such downloading would occur repeatedly, from time to time. As such, a POSITA would have understood, or at minimum found it obvious, that temporary commercial transaction rewriting keys are downloaded periodically.¹⁰ This is consistent with iCashe’s infringement contentions, in which the downloading is allegedly performed from time to time.¹¹ Dreifus ¶153. As discussed in §IX.A.3, a POSITA would have been motivated to apply Abe’s teachings of downloading temporary transaction information to Doughty’s telecommunications device. Dreifus ¶¶154. • Fig. 24:

¹⁰ Ex. 1042, 921.

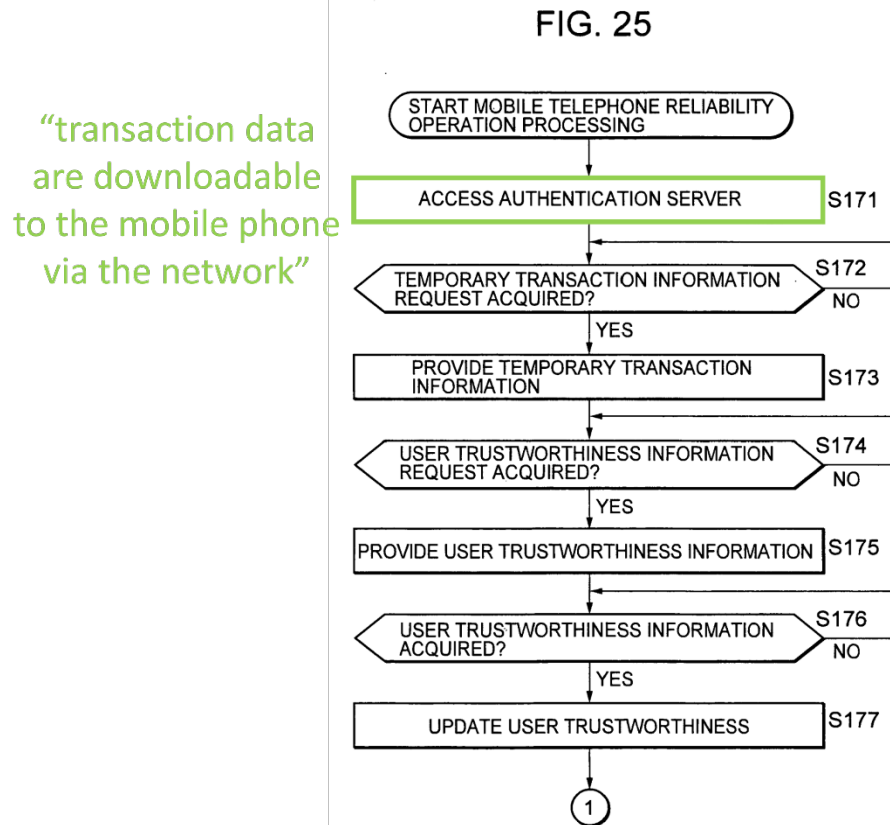
¹¹ Ex.1014, Appx.H-1, 81-84.

'174 Claim

Doughty (US2004/0133787) in view of Abe (US2005/0086171)



• Fig. 25:



'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0187]: “<i>The temporary commercial transaction information rewriting key 362 is key information for making, editing and deleting etc. temporary commercial transaction information. The temporary commercial transaction information rewriting key 362 is a kind of one-time password and is supplied to the mobile telephone 11 etc.</i> while the point-of-receipt server 31 authentication server 41 generating the temporary commercial transaction information rewriting key 362 update the temporary commercial transaction information....The point of receipt server 31 and the authentication server 41 generating the temporary commercial transaction information rewriting key 362 can supply temporary commercial transaction information rewriting keys 362 to the mobile telephone 11 any number of times.” • [0329]: “As described in the following, <i>the authentication server 41 that has acquired the notification of completion of writing provides a temporary commercial transaction information rewriting key 362 to the mobile telephone 11,</i> and instructs the deletion of the temporary commercial transaction information 391 stored in the non-contact IC card 146.” • [0330]: “In step S182, the main control unit 131 <i>determines whether or not an instruction to delete the temporary commercial transaction information has been acquired via the antenna 112, and waits until it is determined that acquisition has taken place.</i>” • [0484]: “First, in step S471, <i>as in the case of step S171 of FIG. 25, the main control unit 131 of the mobile telephone</i>

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	<i>11 accesses the authentication server 41 via the network 10.”</i>
[9] The mobile phone of claim 1, wherein the transaction data includes a transaction number used for each transaction of the plurality of transactions.	<i>See [1].</i> Abe discloses that the transaction data (<i>e.g.</i>, transaction data received from “authentication server 41”) includes a transaction number used for each transaction of the plurality of transactions (<i>e.g.</i>, “card identification number 351”). <u>E.g., Abe</u> <i>See [1.a], [1.c].</i> Abe discloses that the “card identification number 351” included in the downloaded transaction data is provided to a point-of-purchase or point-of-receipt server during the course of a transaction. [0197], [221], [0245], Fig. 12, 17.¹² The card identification number 351 identifies the “non-contact IC card” that is performing the transaction. [0179]. Because the card identification number identifies the IC card, and is provided during each individual transaction, it is used for each of a plurality of transactions. [0179]. Dreifus ¶¶155-158. As discussed in §IX.A.3, a POSITA would have been motivated to apply Abe’s teachings of downloading transaction data to Doughty’s telecommunications device. Dreifus ¶159. • Fig. 12:

¹² The identification of a card number as a transaction number is consistent with iCashe’s infringement contentions, in which the transaction number is allegedly “card information.” Ex.1014, Appx.H-1, 84-86. Dreifus, ¶158.

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	FIG. 12 The diagram illustrates a transaction system involving three main components: an AUTHENTICATION SERVER (41), a MOBILE TELEPHONE (11), and a POINT-OF-PURCHASE SERVER (21). The AUTHENTICATION SERVER (41) includes a STORE TRUSTWORTHINESS module (323, 354). The MOBILE TELEPHONE (11) contains a NON-CONTACT IC CARD (146) which includes: - USER TRUSTWORTHINESS (352) - CARD IDENTIFICATION NUMBER (351), highlighted with a blue border and labeled as the <i>"transaction number"</i>. - PURCHASING INFORMATION (353) containing: • PURCHASING IDENTIFIER • PAYMENT IDENTIFIER • IDENTIFICATION NUMBER FOR PURCHASING CARD The POINT-OF-PURCHASE SERVER (21) includes a PURCHASING INFORMATION module (353) containing: - PURCHASING IDENTIFIER - PAYMENT IDENTIFIER - IDENTIFICATION NUMBER FOR PURCHASING CARD Communication is shown via arrows: - 371: From Mobile Telephone to Authentication Server. - 372: From Authentication Server to Mobile Telephone. - 373: From Mobile Telephone to Point-of-Purchase Server. - 374: From Point-of-Purchase Server to Mobile Telephone. - 375: From Mobile Telephone to Point-of-Purchase Server. - 376: From Point-of-Purchase Server to Mobile Telephone. - 377: From Mobile Telephone to Point-of-Purchase Server. - 378: From Point-of-Purchase Server to Mobile Telephone. - 379: From Mobile Telephone to Point-of-Purchase Server. - 380: From Point-of-Purchase Server to Mobile Telephone. • Fig. 17:

'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	FIG. 17 <pre> graph TD 1((1)) --> S71[REQUEST CARD IDENTIFICATION NUMBER INFORMATION S71] S71 --> S72{CARD IDENTIFICATION NUMBER INFORMATION ACQUIRED? S72} S72 -- NO --> S72 S72 -- YES --> S73[EXECUTE PURCHASING/CHARGE PROCESSING S73] S73 --> S74[PROVIDE PURCHASING INFORMATION S74] S74 --> S75{NOTIFICATION OF WRITING COMPLETION ACQUIRED? S75} S75 -- NO --> S75 S75 -- YES --> S76[PROVIDE NOTIFICATION OF PROCESSING COMPLETION S76] S76 --> S77{COMPLETE? S77} S77 -- YES --> END([END]) S77 -- NO --> 3((3)) 2((2)) --> S77 </pre> “transaction data for use in a plurality of transactions” [0197]: “The point-of-purchase server 21 that has acquired the user trustworthiness 352 and confirmed that the user of the mobile telephone 11 is trustworthy then makes a request to the mobile telephone 11 for the card identification number 351 allotted to the non-contact IC card 146 (arrow 376). <i>The mobile telephone 11 then provides the card identification number 351 in response to this request.</i>”

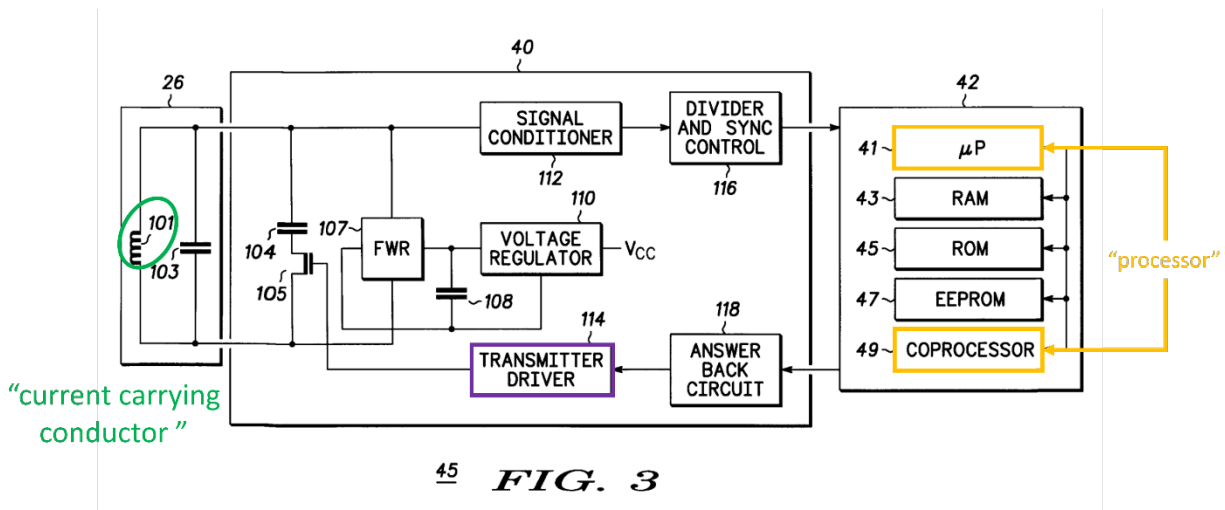
'174 Claim	Doughty (US2004/0133787) in view of Abe (US2005/0086171)
	• [0221]: “In step S25, the main control unit 131 determines whether or not a request for this card identification number information has been acquired, and waits until it is determined that acquisition has taken place. <i>When it is determined that a card identification number information request has been acquired, the main control unit 131 advances processing to step S26, the card identification number 351 is acquired from the non-contact IC card 146, and card identification number information containing this card identification number 351 is provided to the point-of-purchase server 21 via the network 10.</i> This processing corresponds to the processing of arrow 377 of FIG. 12.” • [0245]: “To conform with this request, in step S26 of FIG. 14, the main control unit 131 of the mobile telephone 11 supplies card identification number information to the point-of-purchase server 21.”

B. Ground 2: Doughty in View of Abe and Fox (Claims 1-9)

To the extent it is argued that further disclosure is required of “a (current) driver to excite the current carrying conductor,” and “a processor coupled to control the driver” ([1.d], [1.e], and [6]) **Doughty** in view of **Fox** renders obvious these limitations. Dreifus ¶160.

Fox discloses a “cellular telephone 10” that includes a “smartcard function” including an “RF interface” providing a “contactless interface between the smartcard logic function circuitry in telephone 10 and an external reader/system.” Fox,

2:10-29. The disclosed RF interface includes a “smartcard antenna 26” that “may take the form, for example, of capacitor 103 and a wire such as inductor 101.” Fox, 3:49-59, Fig. 3. The current to the inductor is controlled by “transmitter driver 114” when “information is transmitted out of the smartcard.” Fox, 3:49-59, Fig. 3. Smartcard logic function circuitry (including microprocessor 41 and coprocessor 49) are coupled to control the transmitter driver. Fox, 3:49-59, 4:43-56, Fig. 3; Dreifus ¶161.



Fox discloses a current driver (e.g., “transmitter driver 114”) to excite the current carrying conductor (e.g., “inductor 101”). See, e.g., Fox, 3:49-59, Fig. 3. For example, Fox discloses that smartcard antenna 26, which transmits a time-varying magnetic field (“transmission and reception of RF data”), includes inductor 101 and capacitor 103. Fox, 3:49-59. In order to transmit data from a smartcard, the “transmitter driver 114” adjusts the resonance frequency of capacitor 103 and

inductor 101 by controlling capacitor 104 and FED switch 105. Fox at 3:49-59, Fig. 3. Dreifus ¶162.

Fox discloses a processor (*e.g.*, “microprocessor 41” and/or “coprocessor 49”) **coupled to control the driver** (*e.g.*, coupled to “transmitter driver 114” as illustrated in Fig. 3 to perform “smartcard functions” via “transmitter driver 114”). *See, e.g.*, Fox, 3:49-59, Fig. 3. For example, **Fox** further discloses that smartcard logic function circuitry 42 (containing microprocessor 41 and coprocessor 49) controls “transmitter driver 114” to modify the resonance of inductor 101 and capacitor 103 via capacitor 104 and FED switch 105. Fox, 3:49-59. To perform this control, as illustrated in Fig. 3, microprocessor 41 and/or coprocessor 49 is coupled to transmitter driver 114 via answer back circuit 118. Dreifus ¶163.

Like Doughty and Abe, Fox is analogous art, in the same field as the ’174, which includes electronic devices for performing transactions, and are reasonably pertinent to purported problems addressed by the named inventors of the ’174 patent involving the use of electronic devices to securely perform transactions. Fox, 1:5-8, 2:10-29, 3:49-59, 4:43-56, Fig. 3; Dreifus ¶164.

A POSITA would have been motivated to apply **Fox’s** teachings of a transmitter driver that drives an inductor to **Doughty’s** telecommunications device to excite **Doughty’s** inductive coil 552 to produce a time-varying magnetic field as

desired by **Doughty**. Dreifus ¶165. For example, while **Doughty** discloses that its inductive coil 552 is “pulsed with varying currents and current directions” to produce a time-varying magnetic field, it does not expressly provide details of how the coil is driven to do so, and a POSITA would have looked to **Fox** for such implementation details. **Doughty**, [0051]; Dreifus ¶165. **Fox** teaches such details by disclosing a transmitter driver 114 to drive current to a smartcard antenna for emitting a magnetic field. **Fox**, 3:49-59, Fig. 3; Dreifus ¶165.

Further, a POSITA would have been motivated to apply **Fox’s** teachings of a processor to control a driver in implementing **Doughty’s** telecommunication device (as modified by **Abe’s** teachings) to control the production of a time-varying magnetic field. Dreifus ¶166. While **Doughty** teaches the generation of a time-varying magnetic field, **Doughty** does not explicitly identify what controls the disclosed varying current and current directions in inductor coil 552. **Doughty**, [0051]. A POSITA would have looked to **Fox’s** teachings of a processor, such as microprocessor 41 and/or coprocessor 49, to control transmitter driver 114 based on information that is to be transmitted by the antenna. **Fox**, 3:49-59, 4:43-56, Fig. 3; Dreifus ¶166.

A POSITA would have found it straightforward and advantageous to apply **Fox’s** teachings of a transmitter driver to drive current to an inductor and a processor

to control the driver to **Doughty**'s telecommunications device (as modified by Abe's teachings) to implement the functionality described in **Doughty**. Dreifus ¶167. A POSITA would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶167.

C. Grounds 3-4: Grounds 1-2 in Further View of Dua (Claim 7)

To the extent it is argued that further disclosure is required that **Abe**'s "network 10" is one of a cellular network or a wireless local area network, **Dua** **discloses a network that is one of a cellular network** (*e.g.*, "2.5G" or "3G") **or a wireless local area network** (*e.g.*, "Wi-Fi"). Dua, [0026], [0104]. Dreifus ¶168.

Dua discloses a system for conducting "financial and other transactions requiring authorization" and discloses that "credentials are ultimately supplied to a handheld device such as a mobile telephone via a wireless network." Dua, [0026]. Further, the system disclosed in **Dua** is "designed to interoperate with mobile 2.5G, 3G, and Wi-Fi networks among others." Dua, [0104]. **Dua** therefore discloses a system in which transaction data, such as transaction data is downloadable to a mobile phone via a cellular (2.5G or 3G) or wireless local area (Wi-Fi) network. Dua, [0026], [0104]; Dreifus ¶169.

Like **Doughty**, **Abe** and **Fox**, **Dua** is analogous art, in the same field as the '174, which includes electronic devices for performing transactions, and is reasonably pertinent to purported problems addressed by the named inventors of the

'174 patent involving the use of electronic devices to securely perform transactions using a network. Dua, [0026], [0104]; Dreifus ¶170.

A POSITA would have been motivated to apply **Dua's** teachings of using a cellular or wireless local area network to the downloading of transaction data over a network as taught in **Abe** in implementing **Doughty** (as modified by Abe's teachings and optionally modified by Fox's teachings). Dreifus ¶171. For example, a POSITA would have understood that cellular and wireless local area networks were common networks used for communication in order to advantageously improve the available usage of the telecommunications device. Ex.1041, [0085], [0088], [0091]. Dreifus ¶171.

A POSITA would have found it straightforward and advantageous to apply **Dua's** teachings of a cellular or wireless area network to **Abe's** disclosure of downloading transaction data over a network in implementing **Doughty** (as modified by Abe's teachings and optionally modified by **Fox's** teachings). Dreifus ¶172. A POSITA would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶172.

D. Grounds 5-6: Grounds 1-2 in Further View of Flitcroft (Claim 8)

To the extent it is argued that further disclosure is required that downloaded transaction data is valid for a limited number of transactions and one or more parts of the transaction data is downloaded periodically, **Flitcroft discloses downloaded**

transaction data (*e.g.*, “downloaded” “credit card numbers”) **is valid for a limited number of transactions** (*e.g.*, “limited use”) **and the one or more parts of the transaction data is downloaded periodically** (*e.g.*, supplied “monthly”). Flitcroft 5:5-19, 7:55-66, 10:36-51, 14:12-29. Dreifus ¶173.

Flitcroft discloses a credit card system in which “limited-use credit card numbers” are employed that can be deactivated upon a “limited-use event” such as when “the limited-use credit card is used to accrue charges which are greater than a prescribed monetary amount, which are greater than a prescribed frequency of use, and/or a combination of use frequency, individual transaction amount and total amount.” Flitcroft, 5:5-19. For example, “the multiple use credit card number could be limited to, for example, five uses with a credit limit not exceeding \$100 in each transaction and an aggregate credit limit not exceeding \$400.” Flitcroft, 7:55-66. Additionally, the limited-use credit card can be “downloaded to a radio unit 140 (such as a portable telephone) via wireless communication.” 10:48-51. Dreifus ¶174.

Flitcroft further discloses that a set of limited-use credit card numbers can be provided “in a monthly or other periodic account statement sent to the customer.” Flitcroft, 10:26-56; Dreifus ¶175.

Like **Doughty, Abe and Fox**, **Flitcroft** is analogous art, in the same field as the '174, which includes electronic devices for performing transactions, and is

reasonably pertinent to purported problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions using a network. Flitcroft 5:5-19; 10:26-56. Dreifus ¶176.

A POSITA would have been motivated to apply **Flitcroft's** teachings of downloading limited-use credit card numbers periodically to **Doughty's** telecommunication device (as modified by **Abe** and optionally modified by **Fox's** teachings). Dreifus ¶177. A POSITA would have understood that downloading limited-use credit card numbers periodically would advantageously improve the security of the telecommunications device by ensuring that the card number could not be used if it is obtained later, or that its use would be limited in time or by number of uses, thereby minimizing the amount of money that is improperly transacted with the account number.¹³ Flitcroft, 7:37-54; Dreifus ¶177.

A POSITA would have found it straightforward to apply **Flitcroft's** teachings of limited-use credit card numbers downloaded periodically to **Doughty's**

¹³ **Flitcroft's** "limited-use credit card numbers" are different than **Abe's** temporary rewriting keys in that **Flitcroft's** credit card numbers are used to identify a credit account, while **Abe's** rewriting keys are used to prevent duplication or falsification of temporary commercial transaction information. Flitcroft, 6:53-64, 10:67-11:14; Abe, [0186]. Dreifus, ¶177.

telecommunication device (as modified by **Abe** and optionally modified by **Fox's** teachings). Dreifus ¶178. A POSITA would have known that the combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶178.

E. Grounds 7-8: Grounds 1-2 in further view of Bursch (Claim 9)

To the extent it is argued that further disclosure is required of a transaction number used for each transaction of the plurality of transactions, **Bursch discloses a transaction number used for each transaction of the plurality of transactions** (e.g., “single-use, transaction number”). Bursch, Abstract, 2:22-32, 2:65-67, 5:53-60. Dreifus ¶179.

Bursch discloses methods for producing and applications for using “single-use, transaction numbers” to “make purchases of good and services.” *See, e.g.*, Bursch, Abstract, 2:22-32, 2:65-67, 5:53-60, 5:61-65, 7:55-8:3. These transaction numbers are “single-use” because they are “only valid for a single transaction.” Bursch, Abstract, 2:22-32, 5:53-60, 5:61-65. The “single-use transaction numbers” may be generated using a “transaction number generator” that “may be implemented in handheld devices” including “for example, a PDA or a telephone.” Bursch, 7:50-54, 3:61-62. Dreifus ¶180.

Like **Doughty, Abe, Fox, and Flitcroft**, **Bursch** is analogous art, in the same field as the '174 patent, which includes electronic devices for performing

transactions, and is reasonably pertinent to alleged problems addressed by the named inventors of the '174 patent involving the use of electronic devices to securely perform transactions using a network. Bursch, 1:6-9, 1:13-2:18, 2:22-44, 5:66-6:10, 6:26-52, 7:50-54. For example, **Bursch** discloses methods of performing secure financial transactions in mobile devices. Bursch 5:53-60, 5:60-65, 7:50-54. Dreifus ¶181.

A person of ordinary skill in the art would have been motivated to apply **Bursch's** teachings of single-use transaction numbers to **Doughty's** user device (as modified by **Abe** and optionally modified by **Fox's** teachings) such that the single-use transaction number would be transmitted with **Doughty's** disclosed binary data to enable a transaction in order to advantageously improve the security of its financial transactions. Dreifus ¶182. For example, **Doughty** explains that its user device is intended to "improve the effectiveness and security of a given card or device." Doughty, [0003], [0004], [0008]. **Bursch** discloses that its transaction numbers improve security because they "can be generated just prior to being used," which "minimiz[es] the amount of time during which they can be lost or stolen." Bursch, Abstract, 5:61-65. Further, the transaction numbers are secure because they are generated using "encryption technology" that makes it "very difficult if not impossible to predict what the next transaction number generated will be." Bursch,

Abstract. The transaction numbers are “unique to [each] user” and can be “validated or authenticated by an issuing institution” or other party. Bursch, Abstract. Further, **Bursch** discloses that the use of “single-use transaction numbers” further improves security by allowing for a “variety of invalidation actions” to be initiated if “the expected transaction number does not match the transaction number received. Bursch, 4:50-54. Dreifus ¶182.

A person of ordinary skill in the art would have found it straightforward and advantageous to apply **Bursch’s** single-use transaction numbers teachings to **Doughty’s** telecommunications device (as modified by **Abe** and optionally modified by **Fox’s** teachings) and would have known such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Dreifus ¶183.

X. SECONDARY CONSIDERATIONS

There is no evidence in the ’174’s prosecution history or elsewhere supporting any secondary considerations arguments, or evidence of nexus to any challenged Claim. *See generally* ’174FH; Dreifus ¶185. Indeed, as demonstrated by the prior art referenced herein, any purported solutions to problems or unexpected results in the ’174 were already well known. Dreifus ¶184.

To the extent that PO contends that the accused products in the Texas Case are infringing and thus demonstrate commercial success, any such conclusory

allegations would fail to provide any indication that the Claims are non-obvious. Such conclusory assertions would not demonstrate that Samsung's products infringe, let alone show any nexus between any alleged commercial success and the Claims, or that any alleged success is due to an allegedly claimed component instead of the many unclaimed features of the accused products. Dreifus ¶186.

To the extent PO asserts the existence of any secondary considerations in its responses, Petitioners reserve the right to address any such evidence. Dreifus ¶187.

XI. CONCLUSION

Substantial, new, and noncumulative technical teachings have been presented for each Challenged Claim, which are rendered obvious for the reasons set forth above. Dreifus ¶¶188-193. There is a reasonable likelihood Petitioners will prevail as to each of these Claims. *Inter partes* review of Claims 1-9 of the '174 is accordingly requested.

Dated: March 11, 2025

Respectfully submitted,

By: /James L. Davis, Jr./
Name: James L. Davis, Jr.
Registration No. 57,325
ROPES & GRAY LLP

Lead Counsel for Petitioners

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(a) and (d), the undersigned hereby certify that the Petition For *Inter Partes* Review complies with the type-volume limitation of 37 C.F.R. § 42.24(a)(i) because, exclusive of the exempted portions, it contains 13,949 words as counted by the word processing program used to prepare the paper.

Dated: March 11, 2025

Respectfully submitted,

By: /James L. Davis, Jr./

Name: James L. Davis, Jr.

Registration No. 57,325

ROPES & GRAY LLP

Lead Counsel for Petitioners

CERTIFICATE OF SERVICE

I hereby certify that on March 11, 2025, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 11,270,174 and supporting exhibits to be served via express mail on the Patent Owner at the following correspondence address of record as listed on Patent Center:

175023 - MUGHAL GAUDRY & FRANKLIN PC
iCashe, Inc.
1500 NW Bethany Blvd.
Suite 200
Beaverton, OR 97006
UNITED STATES

A courtesy copy was also sent via electronic mail to Patent Owner's litigation counsel at the following addresses:

Fahrenkrog, Aaron R. AFahrenkrog@RobinsKaplan.com;
Drew, Logan J. LDrew@RobinsKaplan.com;
Tremblay, Emily J. ETremblay@RobinsKaplan.com;
Jones, William R. WJones@RobinsKaplan.com;
Viswanathan, Prateek N. PViswanathan@RobinsKaplan.com;
Schmeckpeper, Kia Y. KSchmeckpeper@RobinsKaplan.com;
Andrea Fair andrea@millerfairhenry.com;
Gutierrez, Jessica L. JGutierrez@RobinsKaplan.com

Dated: March 11, 2025

By: /James L. Davis, Jr./
Name: James L. Davis, Jr.
Registration No. 57,325
Lead Counsel for Petitioners