UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC
Petitioner

v.

LIBERTY PEAK VENTURES, LLC
Patent Owner

Case No. IPR2022-00024
U.S. Patent 8,066,181

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 8,066,181

Table of Contents

APPENDIX OF EXHIBITS

Exhibit	Description
1001	U.S. Patent 8,066,181 ('181 Patent)
1002	File History for U.S. Patent 8,066,181 ('181 File History)
1003	U.S. Provisional Application 60/304,216 ("'216 Provisional")
1004	U.S. Patent 7,239,226 ("'226 Patent")
1005	U.S. Provisional Application 60/396,577 ("'577 Provisional")
1006	U.S. Patent 7,889,052 (the "'052 Patent")
1007	U.S. Provisional Application 60/507,803 ('803 Provisional")
1008	Int'l Publication WO 2003/050749 to Wankmueller ("Wankmueller")
1009	U.S. Provisional Application 60/337913 ("Wankmueller-Prov.")
1010	U.S. Patent 6,857,566
1011	U.S. Patent 6,078,888 to Johnson ("Johnson")
1012	U.S. Patent 6,163,771 to Walker *et al*. ("Walker")
1013	U.S. Patent 5,577,121 to Davis *et al.* ("Davis")
1014	U.S. Patent 5,629,981 to Nerlikar ("Nerlikar")
1015	Declaration of Bruce McNair
1016	U.S. Patent 7,735,725 (the "'725 Patent")
1017	U.S. Patent 7,668,750 (the "'750 Patent")
1018	U.S. Patent 7,996,324 (the "'324 Patent")
1019	U.S. Patent 6,130,623 to MacLellan *et al*., filed Dec. 31, 1996 ("MacLellan")
1020	Nadeem Raza *et al.*, *Applications of RFID Technology*, The Institution of Electrical Engineers (1999) ("Raza")
1021	U.S. Patent 5,491,750 to Bellare *et al.*, filed Dec. 30, 1993 ("Bellare")
1022	W. Simpson, *PPP Challenge Handshake Authentication Protocol (CHAP)* RFC (Aug. 1996) ("Simmons"), available at https://www.ietf.org/rfc/rfc1994.txt
1023	John P. McGregor *et al.*, *Performance Impact of Data Compression on*

Exhibit	Description
	Virtual Private Network Transactions, Proc. 25th Annual IEEE Conf. Local Comp. Networks, pp. 500–10 (2000) ("McGregor")
1024	U.S. Patent 3,956,615 to Anderson *et al*., filed June 25, 1974 ("Anderson")
1025	J. Kohl *et al*., *The Kerberos Network Authentication Service (V5)*, RFC 1510 (Sept. 1993) ("Kohl"), available at https://www.hjp.at/(st_a)/doc/rfc/rfc1510.html
1026	S. Bellovin, *Defending Against Sequence Number Attacks*, Network Working Group RFC 1948 (May 1996) ("Bellovin"), available at https://academiccommons.columbia.edu/doi/10.7916/D8MS40P1/download
1027	Declaration of Kevin Jakel

I. INTRODUCTION

Petitioner Unified Patents, LLC ("Unified" or "Petitioner"), respectfully requests *inter partes* review ("IPR") of Claims 1, 2, 4, 6, and 7 (the "Challenged Claims") of U.S. Patent 8,066,181 (the "'181 Patent"). To the best of Unified's knowledge, the '181 Patent is owned by Liberty Peak Ventures, LLC ("Liberty" or "PO").

The Challenged Claims relate to transaction methods in which an RFID device sends an authentication tag to an RFID reader using a random number received from the reader, a tag ID, and a counter value, such as a transaction counter. The patent was allowed based on the use of a counter value to generate the authentication tag. However, the mere idea of using a counter value is a very old concept in both financial transactions and cryptography. The prior art below shows that each limitation of the Challenged Claims is either anticipated or obvious over a combination of analogous art.

II. U.S. PATENT 8,066,181

A. Summary

The ’181 Patent relates to “a system and method for securing a Radio Frequency (RF) transaction using a Radio Frequency Identification (RFID) transaction device,” particularly using an “authentication tag including a random number received from an RFID reader.” *’181 Patent* (EX1001), 1:43-48; *see also* Abstract. An RFID transaction device, such as a fob, communicates information to a point-of-sale (“POS”) device with an RFID reader, which relays the information either directly or indirectly to an account issuer for verification:

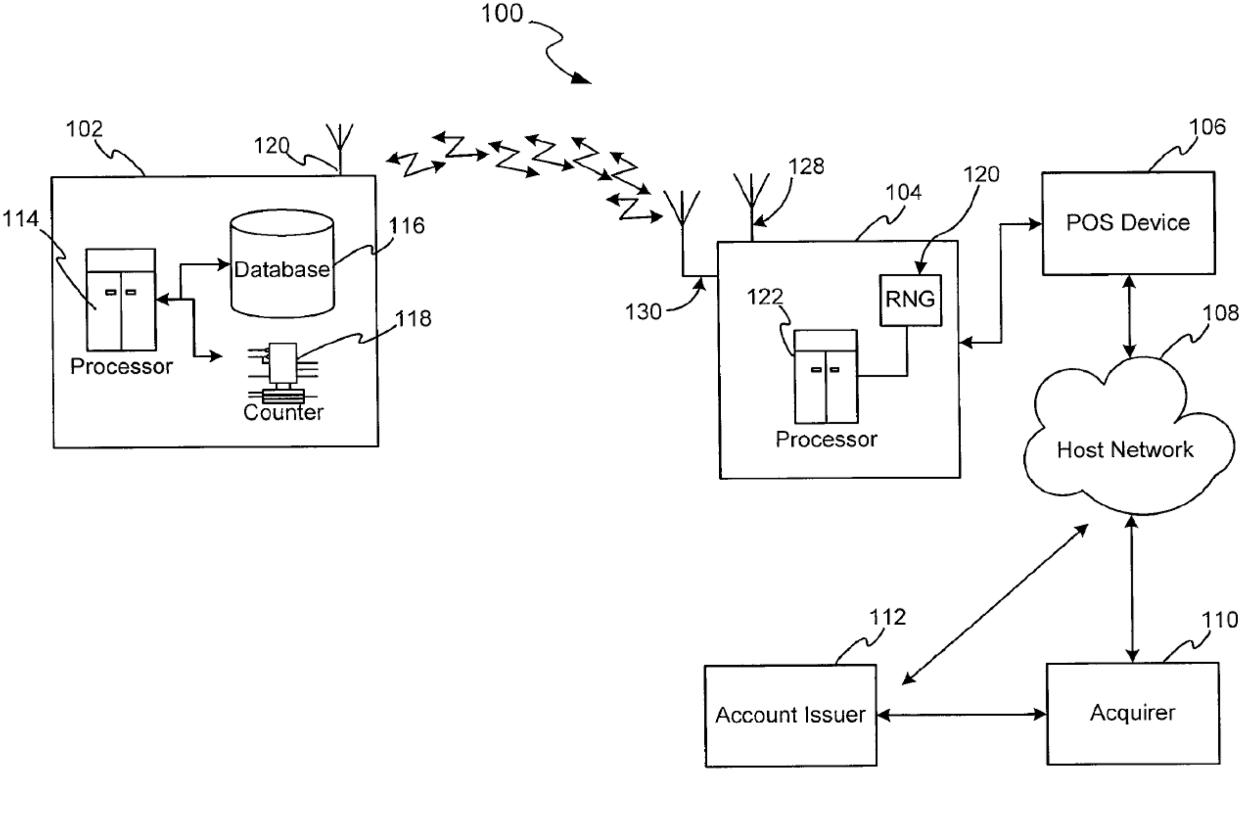


FIGURE 1

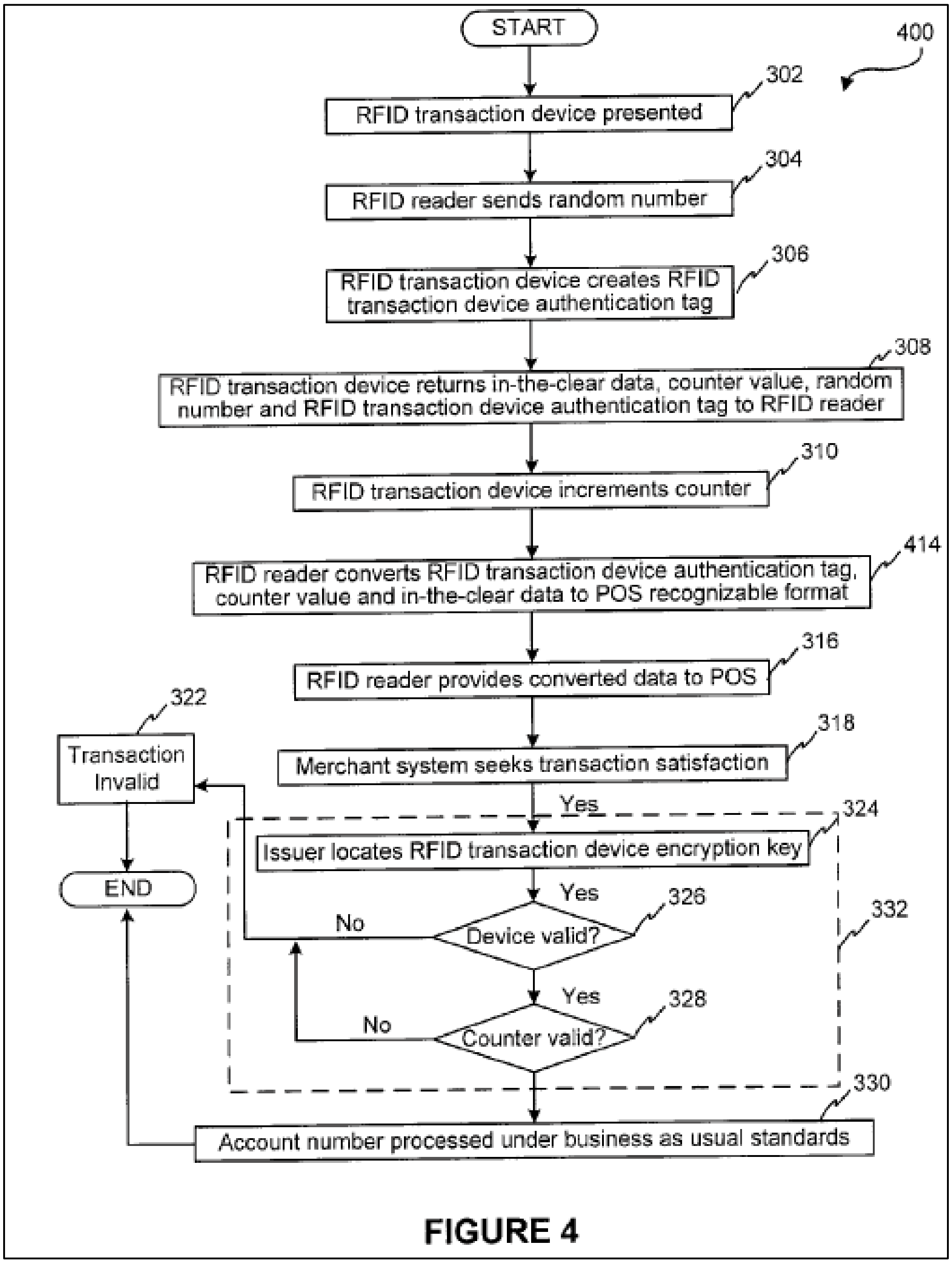
Id., Fig. 1; *see also* 6:26-37 (contemplating the use of "traditional" transponders for transmitting information between the RFID transaction device and reader).

Recognizing the increasing use of RFID technology for completing financial transactions, the '181 Patent sought to address problems such the extra time needed to complete a transaction in order for a user to enter a personal identification number ("PIN") and the risk of theft when a customer's identifying information is sent "in-the-clear." *See id.*, 2:40-3:10. To this end, the specification discloses creating a device "authentication tag" using a random number and other information. *Id.*, Abstract; *see also* 3:20-27. The device may also include a counter for tracking the "number of transactions performed with a particular transaction device." *Id.*, 9:3-5; *see also* 9:44-54. This counter could be a discrete electronic device or a "software or code-based counter as is found in the art." *Id.*, 9:10-12.

The authentication tag may be created using the random number, the counter value, a transaction account number, and a device encryption key. *Id.*, 11:43-51; *see also* 12:43-51.[1] An issuer system may authenticate the data by employing a user's account number to look up an encryption key for decrypting the authentication tag and verifying the user's information. *Id.*, 12:20-34. Figure 4 illustrates one process

[1] The specification discloses other steps irrelevant to the Challenged Claims, such as creating an RFID reader authentication tag.

for validating a user with an authentication tag:


START
400
302
RFID transaction device presented
304
RFID reader sends random number
306
RFID transaction device creates RFID transaction device authentication tag
308
RFID transaction device returns in-the-clear data, counter value, random number and RFID transaction device authentication tag to RFID reader
310
RFID transaction device increments counter
414
RFID reader converts RFID transaction device authentication tag, counter value and in-the-clear data to POS recognizable format
316
RFID reader provides converted data to POS
322
Transaction Invalid
318
Merchant system seeks transaction satisfaction
Yes
324
Issuer locates RFID transaction device encryption key
END
Yes
326
No
Device valid?
332
Yes
328
No
Counter valid?
330
Account number processed under business as usual standards
FIGURE 4

Id., Fig. 4; *see also* Figs. 2, 3, 5-7 (illustrating different embodiments)

The ’181 Patent has four independent claims, two of which are challenged.

Claim 1 describes a method operating from the end-user device perspective:

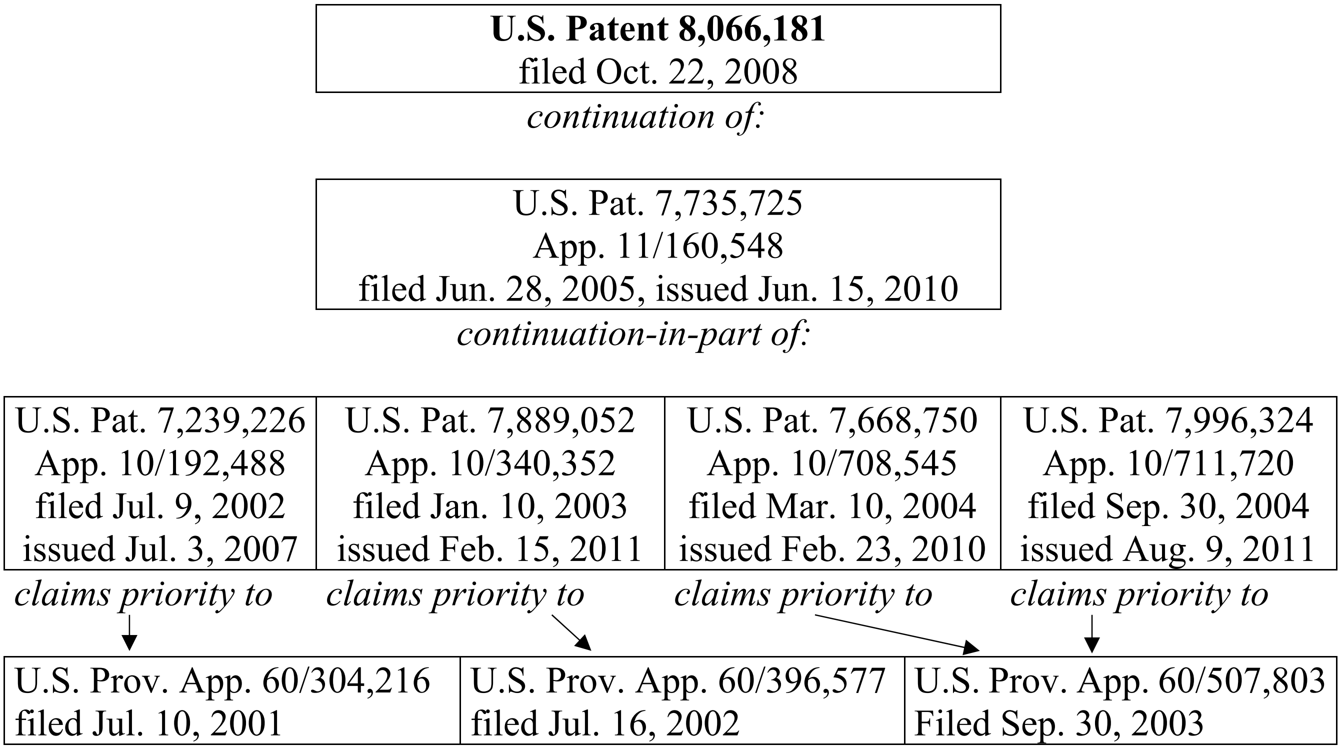
> 1. A method comprising:
>
> generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader;
>
> transmitting the RFID transaction device authentication tag to the RFID reader; and
>
> incrementing the counter value;
>
> wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

Claim 6 is a method claim with similar limitations to Claim 1 but written from the perspective of the RFID reader instead of the end-user device.

B. Priority Date of the '181 Patent

Petitioner challenges the priority claim of the '181 Patent up to at least **September 30, 2003**, as none of the named parent applications filed before this date provide written description or enablement support for the claims of the '181 Patent. The '181 Patent identifies eight related nonprovisional and provisional applications. *'181 Patent* (EX1001), 1:6-39; *see also* (63)-(64). The following chart shows the family chain of applications as described in the '181 Patent:[2]

[2] The '181 Patent describes its chain of priority differently than its parent patents,



U.S. Patent 8,066,181
filed Oct. 22, 2008

continuation of:

U.S. Pat. 7,735,725
App. 11/160,548
filed Jun. 28, 2005, issued Jun. 15, 2010

continuation-in-part of:

U.S. Pat. 7,239,226 App. 10/192,488 filed Jul. 9, 2002 issued Jul. 3, 2007	U.S. Pat. 7,889,052 App. 10/340,352 filed Jan. 10, 2003 issued Feb. 15, 2011	U.S. Pat. 7,668,750 App. 10/708,545 filed Mar. 10, 2004 issued Feb. 23, 2010	U.S. Pat. 7,996,324 App. 10/711,720 filed Sep. 30, 2004 issued Aug. 9, 2011
claims priority to	*claims priority to*	*claims priority to*	*claims priority to*

U.S. Prov. App. 60/304,216 filed Jul. 10, 2001	U.S. Prov. App. 60/396,577 filed Jul. 16, 2002	U.S. Prov. App. 60/507,803 Filed Sep. 30, 2003

If PO intends to claim the priority date of any of its earlier applications for the purpose of traversing any prior art herein, PO should be required to present evidence tending to show that each application in the chain of priority provides written support for the Challenged Claims under 35 U.S.C. § 112 ¶ 1. *Hollmer v. Harari*, 681 F.3d 1351 (Fed. Cir. 2012) ("[I]f any application in the priority chain fails to make the requisite disclosure of subject matter, the later-filed application is not entitled to the benefit of the filing date of applications preceding the break in the priority chain."); *see also Dynamic Drinkware LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378, 1379 (Fed. Cir. 2015) (quoting *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d

and it omits applications to which its parents claim priority.

1316, 1326–27 (Fed. Cir. 2008) (explaining that a patent owner wishing to rebut that an invalidating reference is not prior art because the asserted claim is entitled to the benefit of a filing date must come forward with evidence "'to show not only the existence of the earlier application, but why the written description in the earlier application supports the claim.'").

Here, the earliest parent application named is Provisional Application 60/304216 ('216 Provisional, EX1003), filed July 10, 2001.[3] The '181 Patent does not properly claim priority to the '216 Provisional. None of the flow-chart figures in the '181 Patent are provided in the '216 Provisional. The '216 Provisional makes no mention of the creation of an authentication tag using a random number received from an RFID reader or a counter value, required elements of the independent claims of the '181 Patent. *See '216 Provisional* (EX1003), generally; *see also '181 Patent* (EX1001), Claims 1, 6, 17, 18. Indeed, the '216 Provisional makes no mention of the words "random" or "counter," and Petitioner is unaware of any written description support for these concepts or their equivalents, let alone their use in generating an authentication tag. Further, the '216 Provisional does not provide written description support for incrementing a counter value or an equivalent

[3] Per USPTO records, 117 U.S. patent applications have claimed priority to this provisional application, 71 of which have issued as patents.

concept. Given these missing disclosures, the ’181 Patent does not have priority to the ’216 Provisional. *Lockwood v. American Airlines, Inc.*, 107 F.3d 1565, 1571-72 (Fed. Cir. 1997) (“Entitlement to a filing date does not extend to subject matter which is not disclosed, but would be obvious over what is expressly disclosed. It extends only to that which is disclosed.”). Further, even if the ’216 Provisional did disclose similar concepts to the claimed counter and terminal-originating random number, it does not disclose how a POSA could have used the allegedly similar concepts to generate an authentication tag at an RFID device. *New Railhead Mfg., L.L.C. v. Vermeer Mfg. Co.*, 298 F.3d 1290, 1294 (Fed. Cir. 2002).

The ’181 Patent also does not properly claim priority to U.S. Patent 7,239,226 (the ’226 Patent, EX1004), filed July 9, 2002, U.S. Provisional Application 60/396,577 (the “’577 Provisional,” EX1005), filed July 16, 2002, or U.S. Patent U.S. Pat. 7,889,052 (the “’052 Patent,” EX1006), filed January 10, 2003.[4] The ’226 Patent and the ’577 Provisional lack any mention of a counter, while all three of these applications fail to describe using a counter value to generate an authentication code in an RFID transaction device, as required by each of the independent claims

[4] Only the grounds citing Wankmueller are affected by the ’181 Patent’s priority claims. If Wankmueller has the priority date of its provisional, however, then the priority claims after the ’216 Provisional are moot.

of the ’181 Patent, or incrementing the counter value, as required by Claim 1 and its dependents. Further, even if these applications did disclose similar concepts, they do not disclose how a POSA could have used the allegedly similar concepts to generate an authentication tag at an RFID device. *New Railhead Mfg.*, 298 F.3d at 1294.

The earliest application cited by the ’181 Patent that references both a counter and a random number received from an RF reader and used in the manner claimed is U.S. Provisional Application 60/507,803 (the “’803 Provisional,” EX1007). *See, e.g.*, ’803 Provisional (EX1007), 8-9. Therefore, Petitioner presumes that **September 30, 2003** is the priority date of the ’181 Patent. At this time, Petitioner does not address whether the priority claim to the ’803 Provisional or a later application is otherwise proper.

C. Prosecution History

During prosecution of the ’181 Patent, the original proposed claims were issued without amendment, rejection, or terminal disclaimer. *See ’181 File History* (EX1002), 11-12, 105-06. In a statement regarding the allowable subject matter, the Examiner explained that the closest prior art considered, U.S. Patent 6,073,840 to Marion *et al.*, taught “all of claim 1 **except the inclusion of the counter as part of the response**.” *Id.*, 372. The examiner also discussed U.S. Publication 2004/0257204 to Liao *et al.* and U.S. Publication 2004/0066278 to Hughes *et al.*, observing that neither of these references disclosed the counter limitation.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSA") would have been a person having, as of the priority date of the '181 Patent: (1) at least an undergraduate degree in computer science or closely-related field, or similar advanced post-graduate education; and (2) 1-2 years of experience with systems related to secure communications systems, particularly in the transaction context, where more experience may substitute for less education and vice versa. *See McNair Decl.* (EX1015), ¶¶29-32.

To explain a POSA's knowledge, Petitioner's expert has applied this level of skill for the time period leading up to July 10, 2001. *Id.*, ¶31. However, Mr. McNair notes that, to the extent relevant to the claims of the '181 Patent, a POSA's background knowledge and level of skill would not have substantially changed between July 10, 2001 and September 30, 2003 in a way that would impact the analysis below. *Id.*

E. Claim Construction

Claims are to be construed based on the standards applied by Article III courts (i.e., the *Phillips* standard) in post-grant proceedings. *See* 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). At this time, no construction is necessary for the determination of unpatentability, as the claims are anticipated or obvious under any reasonable construction.

III. REQUIREMENTS FOR *INTER PARTES REVIEW*

A. Standing (37 C.F.R. § 42.104(a))

Petitioner certifies that the ’181 Patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the Challenged Claims.

B. Identification of Challenge and Requested Relief (37 C.F.R. §§ 42.104(b)(1) and 42.22)

In view of the prior art, evidence, and analysis discussed herein, Petitioner requests IPR of Claims 1, 2, 4, 6, and 7 of the ’181 Patent under pre-AIA 35 U.S.C. §§ 102 and 103 based on the following grounds:

Ground	Claims	Challenge
1	1 and 6	Anticipation under § 102 over Wankmueller[5]
2	1, 4, and 6	Obviousness under § 103 over Wankmueller
3	1, 2, 4, 6, 7	Obviousness under § 103 over Johnson[6] and Walker[7]
4	1, 2, 4, 6, 7	Obviousness under § 103 over Johnson, Walker, and Davis[8]
5	1, 2, 4, 6, 7	Obviousness under § 103 over Johnson, Walker, and Nerlikar[9]

[5] Int’l Publication WO 2003/050749 to Wankmueller, EX1008

[6] U.S. Patent 6,078,888 to Johnson, EX1011

[7] U.S. Patent 6,163,771 to Walker *et al.*, EX1012

[8] U.S. Patent 5,577,121 to Davis *et al.*, EX1013

[9] U.S. Patent 5,629,981 to Nerlikar, EX1014

6	1, 2, 4, 6, 7	Obviousness under § 103 over Johnson, Walker, Davis, and Nerlikar

Section II, *supra*, indicates that no constructions for the Challenged Claims are necessary to evaluate the obviousness of these claims. 37 C.F.R. § 42.104(b)(3). Section IV, *infra*, identifies where each element of the Challenged Claims is found in the prior art. 37 C.F.R. § 42.104(b)(4). Numbers and descriptions of Exhibits 1001-1027, attached, are provided above, and the relevance of the evidence to the challenges raised is provided in Section IV. 37 C.F.R. § 42.104(b)(5).

IV. GROUNDS OF UNPATENTABILITY

A. Grounds 1 and 2: Claims 1, 4, and 6 are Anticipated by, and/or Obvious over, Wankmueller

1. Overview of Wankmueller

Wankmueller (EX1008) was filed December 6, 2002, published June 19, 2003, and properly claims priority to a provisional application filed in the United States on December 6, 2001 (discussed in Sec. IV.A.2, *infra*). Thus, Wankmueller is prior art under (i) 35 U.S.C. §§ 102(a) and (e) if the '181 Patent's priority date is later than June 19, 2003 (as Petitioner proposes in II.B, *supra*), (ii) § 102(e) if the '181 Patent's priority date is later than December 6, 2002, and (iii) § 102(e) if the '181 Patent's priority date is later than December 6, 2001 and if Wankmueller has its provisional application's priority date. *See* Sec. II.B, *supra*.

Wankmueller relates to methods and systems for conducting financial transactions using a payment device, such as a card, with two forms of technology, such as a bar code reader and radio frequency communications. *Wankmueller* (EX1008), Abstract, 2:29-3:13; *see also* 6:8-9 ("Preferably, the payment card used in Fig. 2 includes both an optical bar code and an RF ID chip."); 4:16-18; Fig. 1. Wankmueller's use of two technologies was simply meant to be an improvement over the prior art that sent such information using a single machine-readable technology, where identifying information would be sent using a single technology.

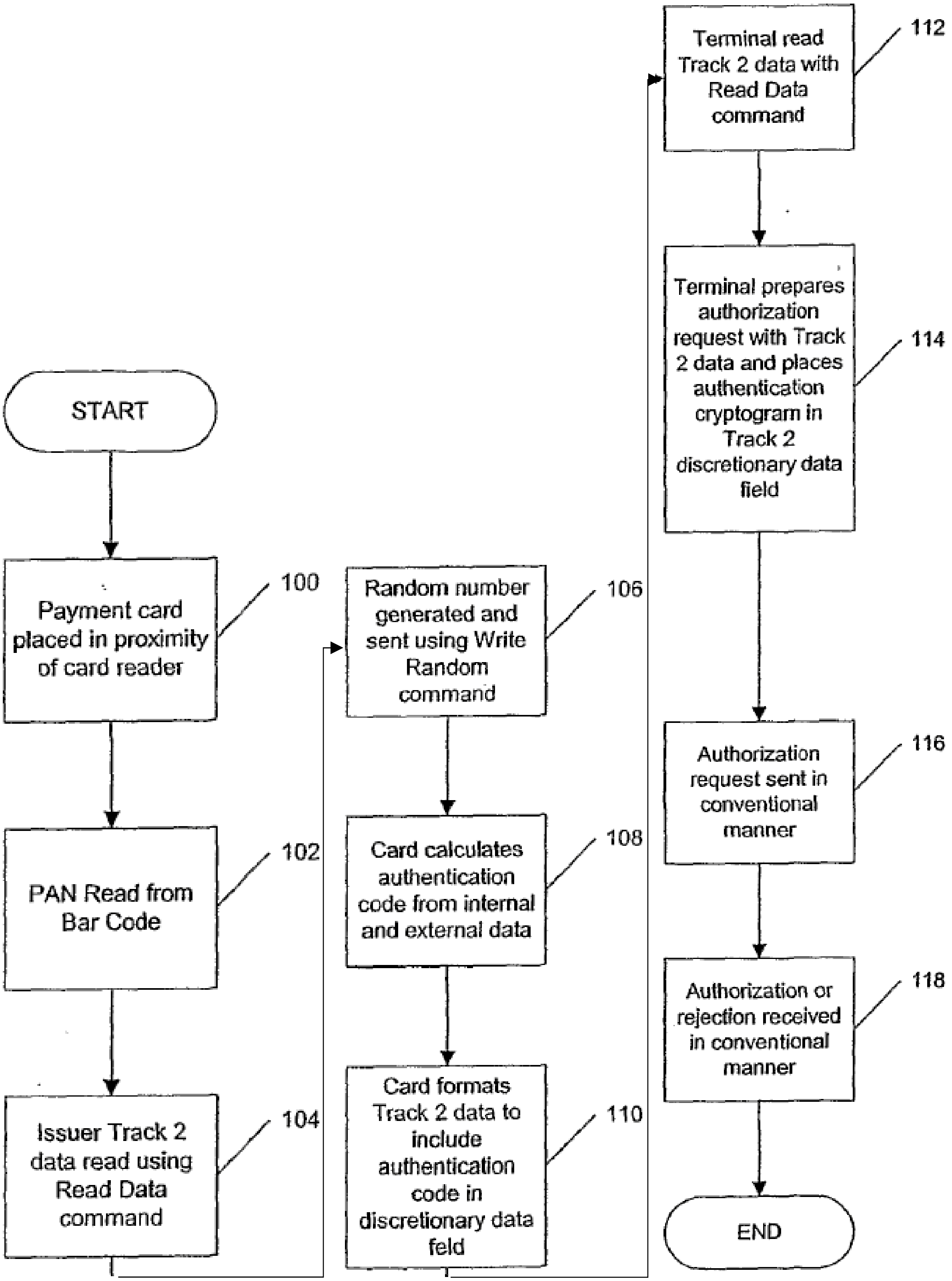
See Wankmueller (EX1008), 2:4-17; *see also Wankmueller-Prov.* (EX1009), 3. Payment account information needed to conduct the transaction, such as a payment account number (PAN) and an expiration date, is split over the two technologies to make it difficult for a potential thief to skim enough information to conduct a fraudulent transaction. *Id.*, 2:31-3:25; *see also* 4:5-16, 5:32-6:5. To use the payment device, "a conventional point-of-sale (POS) or other payment terminal may be equipped with both an optical bar code reader that reads the bar code on the payment card and an RF receiver to receive the RF information." *Id.*, 5:21-23.

Wankmueller discloses methods of communicating and encoding the information in the RFID portion of the payment device and point-of-sale terminal. An "RF ID" chip on the payment device stores a "unique per-card cryptographic key," supports a "cryptographic algorithm to calculate an authentication code," maintains and increments a transaction counter, stores certain payment data from an issuer, and executes certain Read and Write commands when in communication with a POS terminal. *Id.*, 6:8-7:10.

To perform a transaction, part of the payment authentication information is read from the bar code, and the RF chip portion receives a challenge number, which may be a random or fixed value, from the POS terminal. *Id.*, 6:22-30; *see also* 8:29-9:5. Wankmueller discloses that the payment account information may be sent in "any manner" as long as it would not compromise the user's account. *Wankmueller*

(EX1008), 5:32-6:3 ("While a preferred distribution for payment account information has been described, **payment account information may be distributed in any manner between the two technologies on the payment card**, so long as the reading of the account information stored in one technology does not compromise the account ... [I]t is preferred that the PAN and expiry date not be readable using the same technology."); 3:4-6 ("The payment account information may be split between the two technologies in any manner and the split line may even be ... within the payment account number itself."); 7:11-14 (PAN digits used to calculate authentication code); *see also Wankmueller-Prov*. (EX1009), 7-8, 4. As a POSA would have appreciated from these disclosures, "any manner" would include using all of the PAN in the RF portion of the payment card. *McNair Decl.* (EX1015), ¶54. Alternatively, at least such would have been an obvious variation of Wankmueller's disclosure, given that been a matter of rearranging known elements in a manner consistent with its disclosure and the knowledge and skill of a POSA in a predictable manner. *Id*. For example, in such a case the expiration code and other information to identify the user (e.g., an account name, a device serial number, a portion of the PAN duplicated on the bar code) using the bar code or different technology so that an issuer may apply to correct decryption algorithm. *McNair Decl.* (EX1015), ¶54.

Upon receiving the challenge number, the RF chip increments the transaction counter. *Id.*, 6:24-27, 6:14-17. Then the payment device calculates an authentication code, preferably using DES encryption using a unique cryptographic key, with information such as digits of a payment account number, an expiration date, a service code, the value from the counter, and the challenge number. *Id.*, 7:11-22; *see also* 7:25-8:25 (describing the method of generating the authentication code), 10:1-6. It sends this authentication code to the POS terminal, and then the terminal forwards the authentication code to an issuer for validation. *Id.*, 10:7-24. Figure 2 illustrates an exemplary flow chart of the authorization and authentication process:


START
Payment card placed in proximity of card reader
100
PAN Read from Bar Code
102
Issuer Track 2 data read using Read Data command
104
Random number generated and sent using Write Random command
106
Card calculates authentication code from internal and external data
108
Card formats Track 2 data to include authentication code in discretionary data feld
110
Terminal read Track 2 data with Read Data command
112
Terminal prepares authorization request with Track 2 data and places authentication cryptogram in Track 2 discretionary data field
114
Authorization request sent in conventional manner
116
Authorization or rejection received in conventional manner
118
END

Id., Fig. 2 (reconstructed into three columns for readability).

Wankmueller is analogous art to the ’181 Patent. Wankmueller is within the field of endeavor of the claims of the ’181 Patent because, like the ’181 Patent, it relates to secure financial transactions, particularly those using radio-frequency technology and a random number received from an RFID reader. *See ’181 Patent* (EX1001), 1:43-48; *see also* 1:52-61 (identifying related technologies used in financial transactions, such as barcode and voice data entry); *see also Wankmueller* (EX1008), 4:5-22, 2:29-3:13, 4:27-30; *see also McNair Decl.* (EX1015), ¶¶33, 55. Wankmueller is also reasonably pertinent to multiple problems concerning the inventor of the ’181 Patent, such as (1) the need for a less time-consuming method of conducting RFID transactions and (2) the need to protect a customer’s identifying information from theft. *See ’181 Patent* (EX1001), 2:54-3:16; *see also Wankmueller* (EX1008), 2:26-27 (“Therefore, there exists a need for a payment device and mechanism that is quick, easy, fast and secure and globally interoperable.”); *see also* 1:23-25, 2:13-15, 3:14-25; *see also McNair Decl.* (EX1015), ¶55.

2. Wankmueller’s Priority Date[10]

Wankmueller claims priority to U.S. Provisional Application 60/337913 (“Wankmueller-Prov.,” EX1009), filed December 6, 2001. A patent or printed

[10] The Board need not reach this question if the ’181 Patent lacks priority to either its 2001 or 2002 provisional.

publication has the prior-art date of a parent provisional if (1) the cited portions of the provisional also disclose the claims of the challenged patent, and (2) at least one claim of the prior art patent/publication has written description support in the provisional patent. *See, e.g., Dynamic Drinkware LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378, 1381-82 (Fed. Cir. 2015); *see also Amgen v. Sanofi*, 872 F.3d 1367, 1380 (Fed. Cir. 2017) (*Dynamic* applies to claims of PCT applications).

Here, the specification of Wankmueller and its provisional application are substantively identical—the only changes are the inclusion of the Abstract and minor formatting and word-choice edits. Petitioner provides citations to the provisional in the mapping below showing how it provides support for the portions of Wankmueller used to demonstrate unpatentability of the Challenged Claims.

Additionally, at least one of Wankmueller's claims is supported by its provisional:

Wankmueller Claim 1 (EX1008)	**Wankmueller-Prov. Disclosure (EX1009)**
[1] A system for conducting financial transactions comprising;	*This invention relates to a method and* ***system for conducting financial transactions*** *using payment cards having account information stored therein and readable by two different technologies.* EX1009, 2 (Background of Invention).
[1a] payments cards having stored account information including a first portion readable by a	*According to the presently claimed invention,* ***a payment device includes payment account information that is distributed between two different machine-readable technologies****.*

first machine-readable technology and a second portion readable by a second different machine-readable technology	*Preferably, the payment device according to the presently claimed invention includes one or more digits of a payment account number stored in the payment device in a first machine-readable technology and the remaining digits of the payment account number, if any, and other payment account information stored in the payment device in a second machine-readable technology different than the first machine-readable technology.* ***The payment account information may be split between the two technologies in any manner*** *and the split line may even be (as described above) within the payment account number itself.* *Preferably, the first machine-readable technology is bar-code technology and the second machine-readable technology is radio-frequency (RF) technology.* EX1009, 4 (Summary of the Invention); *see also* 5-6 (Detailed description, similar). *As shown in Fig. 1,* ***the present invention utilizes a payment card 10 with a bar code 20 thereon and radio frequency ID chip or circuitry 30 therein****. ... The bar code is encoded with at least one or more digits of the payment account number (PAN).* ***Preferably, the bar code is encoded with, at a minimum, the most significant digits of the PAN****, including the BIN used to identify the issuer. ...* ***The remaining account information is stored in the RF chip*** *or circuitry 30.* EX1009, 6; *see also* Fig. 1.
[1b] terminals employing both of said first and second technologies to capture said portions of said card account	*To use the card,* ***a conventional point-of-sale (POS) or other payment terminal may be equipped with both an optical bar code reader that reads the bar code on the payment card and an RF receiver to receive the RF***

information for conducting each such transaction	***information**. The information read using the two different technologies from the card is then combined in the reader into regular track data and processed in the same manner as a conventional payment card over existing payment networks.* EX1009, 7; *see also* 11-12 (describing functions of the terminal), Fig. 2.

Further, as Unified's expert testifies, Wankmueller's provisional includes sufficient detail to enable a POSA to make and use Wankmueller's invention by December 6, 2001, as it provides details regarding how to implement its two-technology payment card system and how a developer may program it to generate an authentication code using the information listed and provides a framework for implementing the different methods using existing technologies known to be capable of the concepts described *McNair Decl.* (EX1015), ¶56. Therefore, Wankmueller properly has the prior art date of its provisional application.[11]

[11] The disclosure of Wankmueller's provisional is also nearly identical to a related domestic patent, U.S. Patent 6,857,566 (EX1010). If the provisional application's disclosure were non-enabling, then the domestic counterpart, which includes even narrower claims than Wankmueller, would not have issued.

3. Claim 1

[1P]. A method comprising:

To the extent the preamble is limiting, Wankmueller discloses a method. *Wankmueller* (EX1008), 1:6-9 ("This invention relates to **a method** and system for conducting financial transactions ..."); *see also* 4:5-6; *see also Wankmueller-Prov.* (EX1009), 2, 5.[12]

[1.1]. generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader;

Limitation 1.1 requires that an RFID transaction device generate an **authentication tag** using three pieces of information:

i. **a random number** received from an RFID reader (e.g., a reader of a point-of-sale, or POS, device; *'181 Patent* (EX1001), 7:13-39);

ii. a **transaction device identifier** (e.g., "any identifier for a transaction device which may be correlated to a user transaction account," such as an account number; *id.*, 5:34-43); and

iii. a **counter value** (e.g., a value to track the number of transactions; *id.*, 9:23-

[12] Unless otherwise indicated, all **bold** and color-coded emphasis in quotations has been added, while italics are used to signify claim language.

54, 10:1-7).

The ’181 Patent describes creating this authentication tag using a device encryption key, but it does not otherwise go into detail regarding how the tag is generated. *Id*., 11:43-51; *see also* 12:20-25. The ’181 Patent confirms that the “RFID transaction device and the RFID reader disclosed herein include traditional transponders for transmitting information between the device and the reader.” *Id*., 6:26-39. Further, the counter value may be generated using “a software or code-based counter as is found in the art.” *Id*., 9:6-12.

Wankmueller discloses, or at least renders obvious, limitation 1.1. For example, Wankmueller discloses a payment card that includes an “radio frequency ID chip” or RF chip, that is used to conduct transactions with a point-of-sale terminal that includes an RF reader. *Wankmueller* (EX1008), 4:26-5:9; *see also*, 5:21-23 (“To use the card, **a conventional point-of-sale (POS) or other payment terminal** may be equipped with both an optical bar code reader that reads the bar code on the payment card **and an RF receiver to receive the RF information**.”), 9:22-24; *Wankmueller-Prov.* (EX1009), 4-6, 12.

Using a cryptographic algorithm, the RFID device generates an **authentication code** using, among other information, a **challenge number** received from the POS terminal, all or part of a **payment account number, or PAN**, and a **value from a counter** maintained by the RF chip:

> Preferably, **the RF chip calculates an authentication code for verification by the issuer using its unique cryptographic authentication key and the following data**:
> • **the PAN digits**, if any, from the RF chip Track 2 data;[13]
> • the Expiry Date (4 BCD characters) from the RF chip Track 2 data;
> • the Service Code (3 BCD characters) from the RF chip Track 2 data;
> • **the value from the counter maintained by the RF chip** (preferably, the counter is a minimum of 15 bits); and
> • **the challenge number** (preferably 2 BCD characters) **provided by**

[13] Here, taking digits of the PAN to generate the authentication code is "using" the PAN, as claimed, and neither the specification or the prosecution history suggests that "using" a value requires using each digit of the value in the generation step. Additionally, as discussed above, a POSA would have appreciated that Wankmueller's disclosure teaches or at least render obvious using all of the PAN by storing it in the RF chip circuitry and storing the expiration date with the barcode, as Wankmueller discusses sending payment information in "any manner" across the two technologies as long as it would not compromise the account, thus providing an express teaching, suggestion, or motivation› to employ different arrangements of the payment account information. *Wankmueller* (EX1008), 5:32-6:3, 3:4-6, 7:11-14; *see also Wankmueller-Prov.* (EX1009), 7-8, 4; *McNair Decl.* (EX1015), ¶54; Sec. IV.A.1, *supra*.

the terminal.

Wankmueller (EX1008), 7:11-22; *see also*, 7:23-8:27 (describing preferred embodiments and methods for calculating the authentication code from the above information), 6:8-30 (describing functions of the RF chip), Fig. 2; *see also Wankmueller-Prov*. (EX1009), 8-10, Fig. 2.

Wankmueller explains that the challenge number received from the terminal may be a random number. *Wankmueller* (EX1008), 6:28-29 ("The terminal **challenge number may be a random number** or it may be fixed."), 8:29-9:3 ("Preferably, the terminal in the embodiment of Fig. 2 performs at least the following functions ... **Generate a challenge number** ... either **randomly** or a fixed value ..."), Fig. 2 (step 106); *see also Wankmueller-Prov*. (EX1009), 8-9, 11, Fig. 2 (step 106).

Additionally, just like the '181 Patent, Wankmueller explains that the counter is a transaction counter that generates a value that is incremented based on a predefined event, such as the receipt of a challenge number or before each transaction. *Wankmueller* (EX1008), 6:14-17 and 6:24-27; *see also Wankmueller-Prov*. (EX1009), 8.

Therefore, Wankmueller discloses, or at least renders obvious, this limitation because it discloses the same or equivalent elements used to generate the claimed *authentication tag* to generate its authentication code.

[1.2] transmitting the RFID transaction device authentication tag to the RFID

reader; and

Wankmueller discloses this limitation, or at least renders it obvious. Wankmueller discloses *transmitting the RFID transaction device authentication tag* (e.g., authentication code) to the RFID reader (e.g., the POS terminal):

> In step 108, the RF chip on the payment card calculates an authentication code using its cryptographic key with its internal data (as specified above) and the challenge number sent by the terminal. **In step 110, the RF chip formats the Track 2 data to be sent to the terminal, replacing the discretionary data with the authentication code and other values as specified above. In step 112, the terminal performs a Read Data command and reads the new Track 2 data, including the authentication code**.

Wankmueller (EX1008), 10:1-8; *see also* 6:22-30, Fig. 2 (similar disclosures); 2:17-20, 10:7-12 (RF devices "transmit" data); *see also Wankmueller-Prov.* (EX1009), 3, 12-13, 8-9, Fig. 2.

[1.3] incrementing the counter value;

Wankmueller discloses *incrementing the counter value*, such as before each transaction, or each time a challenge number is presented to the card.

> Preferably, the RF ID chip performs the following functions: ... maintain a transaction counter and **increment the transaction counter before a predefined event, such as before each transaction or after each time a challenge number is presented to the card**.

Wankmueller (EX1008), 6:14-17; *see also* 6:24-27 ("Upon receipt of the challenge number, the RFID device should **increase its transaction counter**, calculate the authentication code, and format Track 2 discretionary data with the chip authentication data."); *see also Wankmueller-Prov.* (EX1009), 8.

[1.4] wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

Wankmueller discloses this limitation, or at least renders it obvious. Specifically, Wankmueller discloses that *an RFID transaction is authorized* (e.g., an authorization response is sent to a terminal allowing a transaction to be completed) *in response to verification of the RFID transaction device authentication tag* (e.g., in response to the terminal verifying the authentication code with an issuing entity that is able to decrypt the information in order to validate the authentication code). Wankmueller discloses that this is accomplished by the POS terminal sending an authorization request to an issuing entity, which derives the unique cryptographic key assigned to the user's account and "validates the authentication code," and it communicates an authorization response (either authorization or rejection) to the POS terminal. *Wankmueller* (EX1008), 10:13-27; Fig. 2 (steps 114-118); *see also Wankmueller-Prov.* (EX1009), 13, Fig. 2.

4. Claim 4

4. The method of claim 1, wherein the counter value is incremented a

predetermined amount.

As discussed, Claim 1 is anticipated by, or at least obvious over, Wankmueller. Further, Claim 4 is obvious over Wankmueller. Wankmueller discloses incrementing the transaction counter before a predefined event, such as "before each transaction" and that the transaction counter value is "maintained by the RF chip." *Wankmueller* (EX1008), 6:8-17, 7:19-20; *see also Wankmueller-Prov.* (EX1009), 8, 9. Wankmueller also discloses that the issuer uses this information to authorize a user's transaction. *See Wankmueller* (EX1008), 8:15-20 (describing that a counter may be converted using different methods provided the conversion is "the same on the issuer system"); *see also* 8:25-27 (issuer allocates the number of characters assigned to the counter); *see also Wankmueller-Prov.* (EX1009), 11. Given *Wankmueller*'s disclosure that the counter is a transaction counter, a POSA would have understood, or at least found obvious that the increment is by a predetermined amount (e.g., one) for each transaction or challenge number received, as that is how transactions would typically be counted. *McNair Decl.* (EX1015), ¶¶46, 52.[14]

[14] Notably, the '803 Provisional of the '181 Patent notes that the "simplest approach" of updating a counter value "is to simply increment the counter by some value." *'803*

5. *Claim 6*

[6P]. A method comprising:

To the extent the preamble is limiting, Wankmueller discloses a method. *Wankmueller* (EX1008), 1:6-9, 4:5-6; *see also Wankmueller-Prov.* (EX1009), 2, 5.

Claim 6 describes limitations similar to those of Claim 1, but from the perspective of the RFID reader instead of the RFID transaction device.

For the same reasons discussed regarding Claim 1 and below, Claim 6 is anticipated by, or at least obvious over Wankmueller. Petitioner notes additional relevant disclosures of Wankmueller below.

[6.1]. generating a random number at a radio frequency identification (RFID) reader;

Wankmueller discloses *generating a random number* (e.g., a challenge number) *at a radio frequency identification (RFID) reader* (e.g., at a point-of-sale (POS) terminal equipped with a bar code reader and RF receiver). *See* Sec. IV.A.3 [1.1.], *supra*; *see also Wankmueller* (EX1008), 8:29-9:3 ("Preferably, the terminal

Provisional (EX1007), 9. The '803 Provisional goes on to say that one "obvious" technique would be incrementing the value by 1, supporting that the incrementation of a transaction counter by some predetermined amount would have been obvious to a POSA. *Id*.

in the embodiment of Fig. 2 performs at least the following functions ... **Generate a challenge number** ... either **randomly** or a fixed value ..."); 6:22-30; *Wankmueller-Prov.* (EX1009), 11, 8.

[6.2]. transmitting the random number to an RFID transaction device; and;

Wankmueller discloses, or at least renders obvious, *transmitting the random number* (e.g., the challenge number) *to an RFID transaction device* (e.g., a payment card or device with a RF chip, also referred to as a Radio Frequency Chip device). *See* Sec. IV.A.3 [1.1.], *supra*; *see also Wankmueller* (EX1008), 9:29-30 ("In step 106, **the terminal sends a Write Data command with a challenge number to the payment card**."); 8:29-9:5, 6:22-24, Fig. 2 (Step 106); *Wankmueller-Prov.*, (EX1009), 11, 12, 8, Fig. 2.

[6.3] receiving, from the RFID transaction device, an RFID transaction device authentication tag, wherein the RFID transaction device authentication tag was generated using a transaction device identifier, a counter value, and the random number.

Limitation 6.3 is similar to limitations 1.1 and 1.2 but written from the perspective of the RFID reader. As discussed regarding limitations 1.1 and 1.2 above, Wankmueller discloses *receiving, from the RFID transaction device* (e.g., a payment card or device with a RF chip, also referred to as a Radio Frequency Chip device)*, an RFID transaction device authentication tag* (e.g., an authentication code)*, wherein the RFID transaction device authentication tag was generated using* *a transaction device identifier* (e.g., all or part of a payment account number, or PAN)*, a counter value* (e.g., a value of a transaction counter)*, and the random number* (e.g., the challenge number). *See* Sec. IV.A.2 [1.1]-[1.2], *supra*; *see also Wankmueller* (EX1008), 5:21-23; *Wankmueller-Prov*. (EX1009), 7.

[6.4] wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

Limitation 6.4 is identical to limitation 1.4. As discussed regarding limitation 1.4, Wankmueller discloses *wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag*. *See* Sec. IV.A.3 [1.4], *supra*; *see also Wankmueller* (EX1008), 10:13-27, Fig. 2 (steps 114-118); *see also Wankmueller-Prov.* (EX1009), 13, Fig. 2.

B. Ground 3: Claims 1, 2, 4, 6, and 7 are Obvious over Johnson and Walker

1. Overview of Johnson

Johnson (EX1011) was filed July 16, 1997 and issued June 20, 2000; thus, Johnson is prior art at least under 35 U.S.C. §§ 102(a), (b), and (e). Johnson relates to systems and methods for providing secure transactions using a tag 100 (interchangeably referred to as a transponder) and a point-of-sale (POS) terminal 200 associated with a host network authorization system 300:

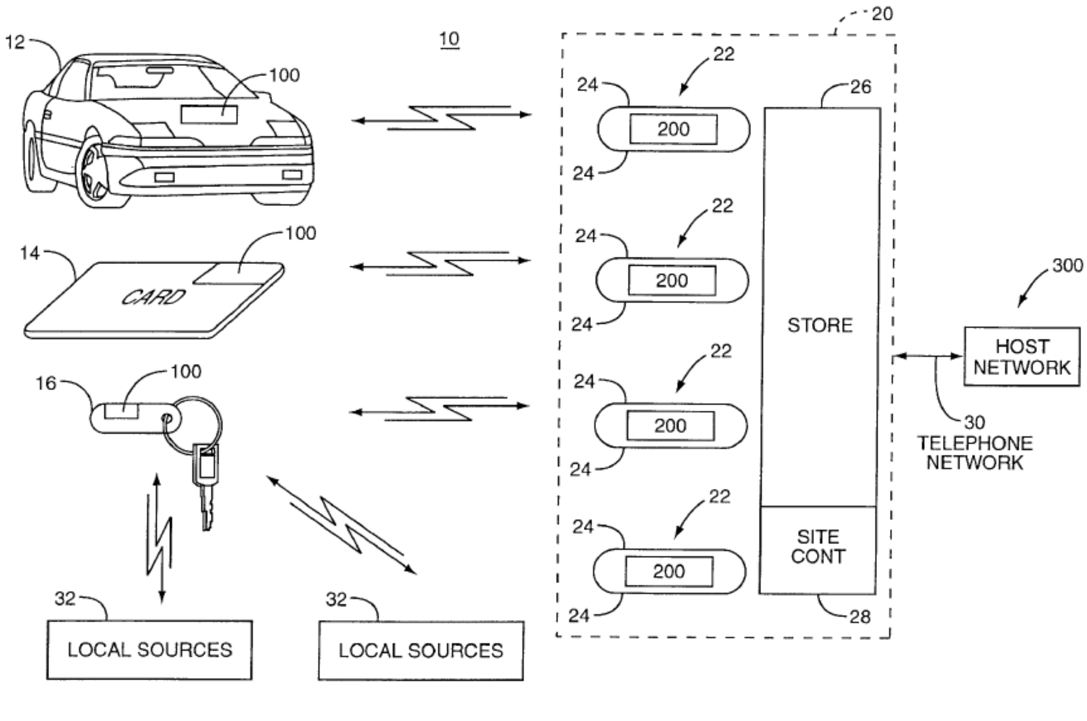


FIG. 1

Johnson (EX1011), Fig. 1; *see also* Abstract, 1:30-35. The tag/transponder is integrated into a carrying medium, such as a transaction card 14 or key fob 16. *See id.*, Fig. 1, 5:66-6:4. To avoid transmitting a user's sensitive financial information, all or a majority of the information is held only at the host network. *Id.*; *see also* 2:61-3:8. The host network derives a unique identifier for each transponder, referred to as the "tag ID," and this number is transmitted to the host through a POS terminal. *Id.*, 3:11-21. The host is able to authenticate the tag "identical cryptography techniques known only by the tag and host, but not by the POS device." *Id.*, 3:22-24. Specifically, the POS device, acting as an "interrogator," will send authentication check data, such as a random number referred to as the "CRN," to the tag. *Id.*, 3:24-

31; *see also* 10:16-19. The tag encrypts the CRN with a main key created by the host and sends the result, referred to as the tag or encrypted random number (ECRN), along with the tag ID to the POS device, which in turn sends the ECRN, the tag ID, and the original CRN to the host. *Id*., 10:19-22; *see also* 3:31-38; *see also* 8:55-65 (describing the host configuring each tag with a tag ID and a preferably unique main tag key); 10:53-62.

Using the information received from the POS device and the information it has stored corresponding to the received tag ID, the host may authenticate the tag in one of two ways: (1) encrypting the original random number (CRN) and comparing the result to the ECRN (*see, e.g.*, *id*., 3:36-44, 10:27-41, 10:63-11:6), or (2) decrypting the ECRN and comparing the result to the original CRN (*see, e.g.*, *id*., 11:6-8). Figure 5 illustrates a preferred tag authentication process:

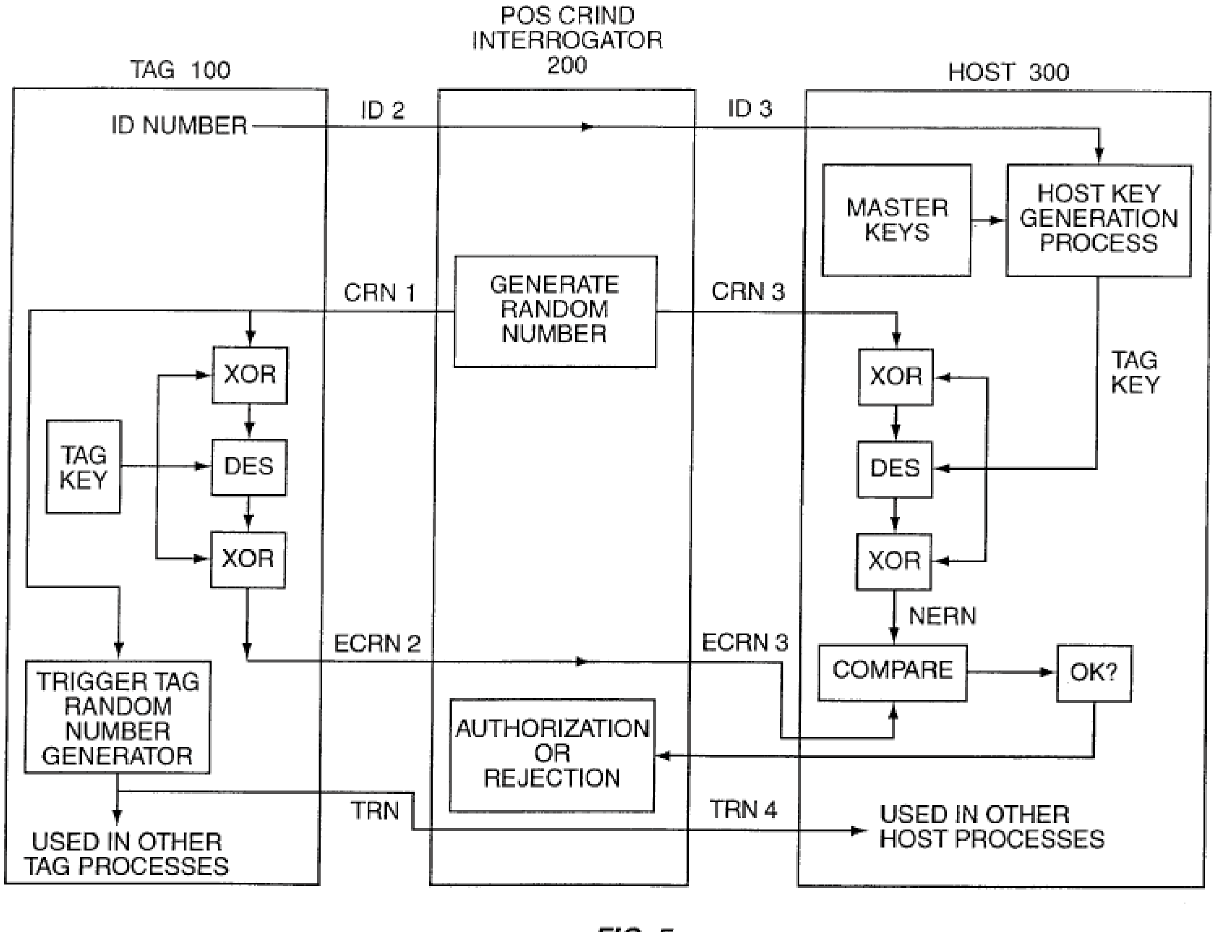


FIG. 5

Johnson is analogous art to the '181 Patent. Johnson is within the field of endeavor of the '181 Patent because it relates to secure financial transactions, particularly RF transaction authentication using a random number. *Id.*, Abstract; *see also* 1:39-46; Claims 1, 7, 13, 29; *see also McNair Decl.* (EX1015), ¶64 (noting that Johnson's terminology is consistent with terms of art used in RFID communications technology); *see also* '181 Patent. Additionally, Johnson is reasonably pertinent to at least one problem concerning the inventor of the '181 Patent. *McNair Decl.* (EX1015), ¶64. Specifically, like the inventor of the '181 Patent, Johnson concerned itself with securing a user's account and financial information from theft. *Johnson* (EX1011), 2:41-55; *see also '181 Patent* (EX1001), 2:63-67.

The concept of using RFID devices and readers in the transactional context is implied by, and at most would have been an obvious variation of, Johnson's description, particularly in light of the ordinary skill and knowledge of a POSA. The '181 Patent itself acknowledges that the use of RFID technology were being used in various automated data collection and identification systems, including for completing financial transactions. *See '181 Patent* (EX1001), 1:52-65. And Johnson itself discloses using tag or transponder and an interrogator of a POS device, which, as a POSA would recognize, are generally terms used to refer to RFID devices, such as key fobs or smart cards. *See McNair Decl.* (EX1015), ¶¶65, 39-43 (citing, e.g., *MacLellan*, EX1019; *Raza*, EX1020). Indeed, Johnson's specification and claims refer to radio frequency transmissions as one means of accomplishing financial transactions. *Johnson* (EX1011), 1:42-44, *see also* 5:66-6:4 (tag is designed to provide "remote bi directional communications" with a POS device). And both the tag and the POS device 200 are depicted with wireless antennas 110 and 112 and 208 for transmitting and receiving information from one another:

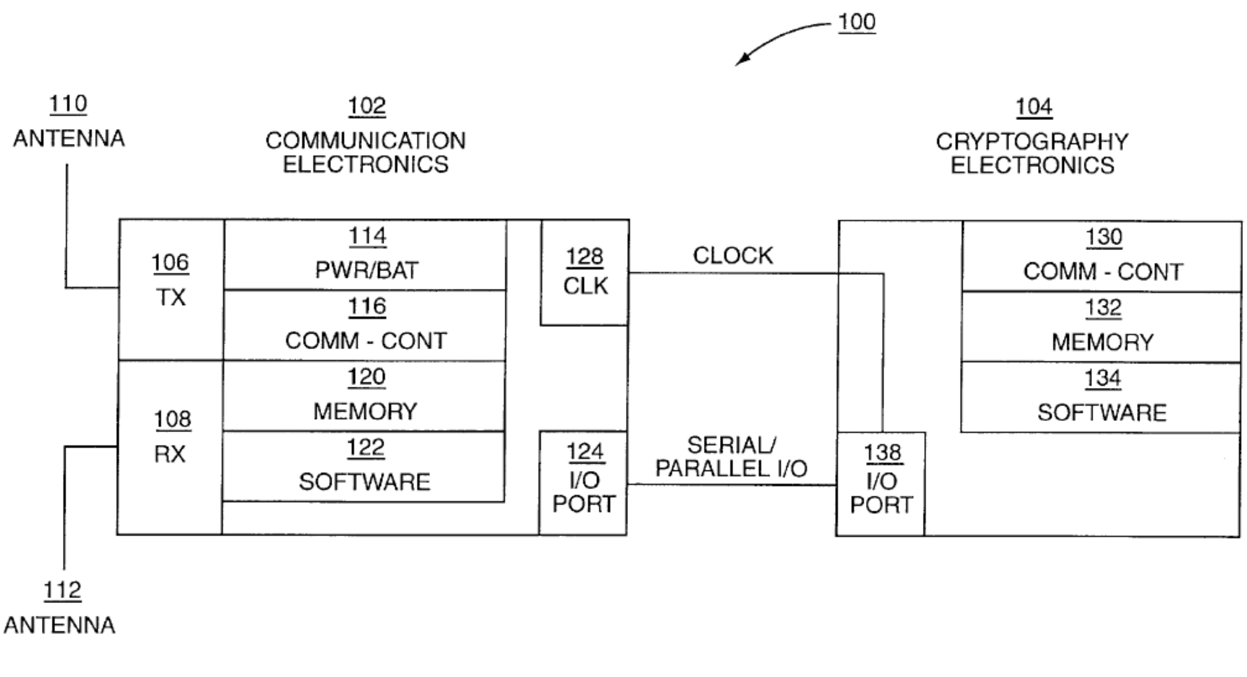


FIG. 2A

Id., Fig. 2A (tag 100); *see also* Fig. 2C (alternative embodiment); *see also* 20:20-25 (tag 100 may be an active tag, i.e., one with its own power source).

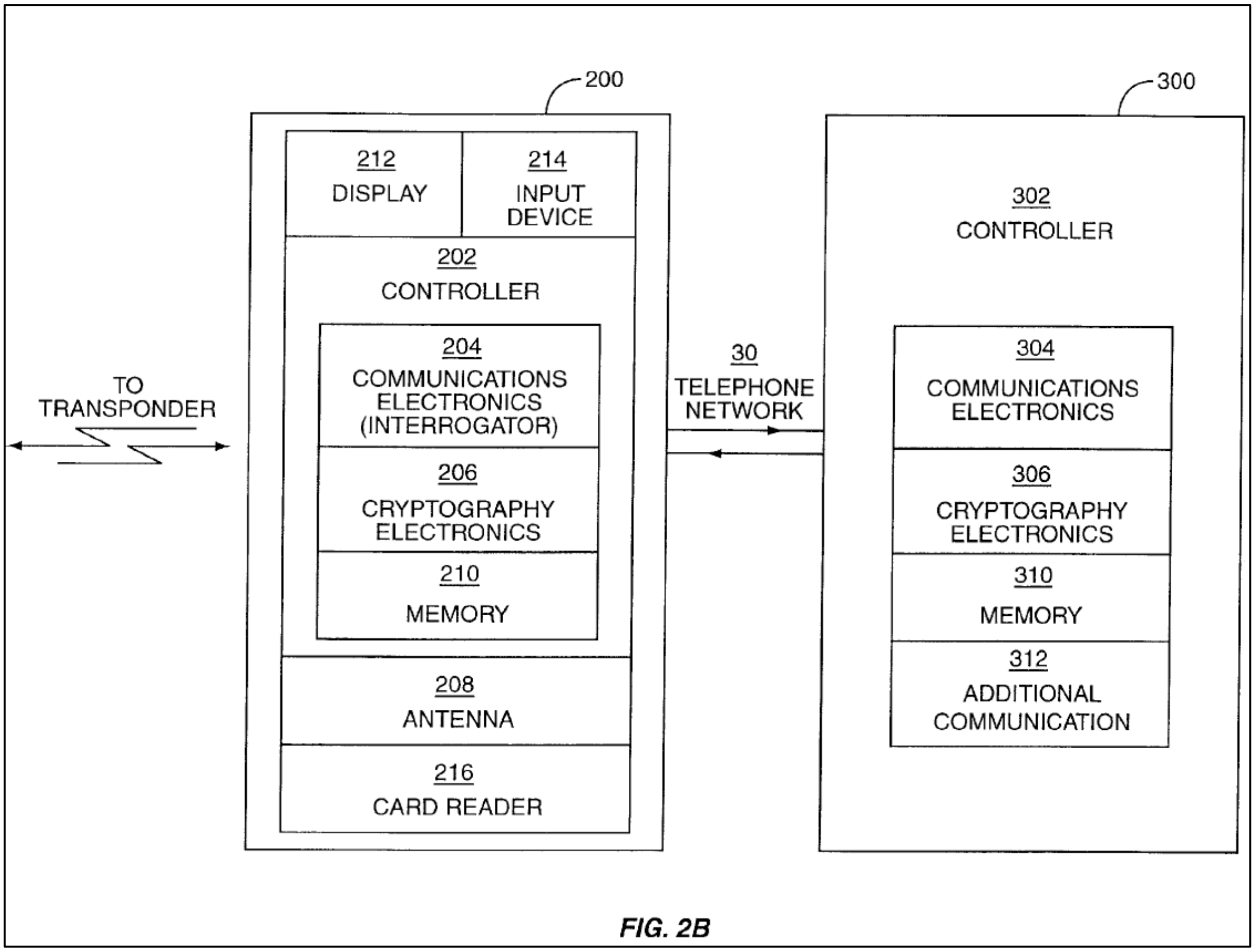
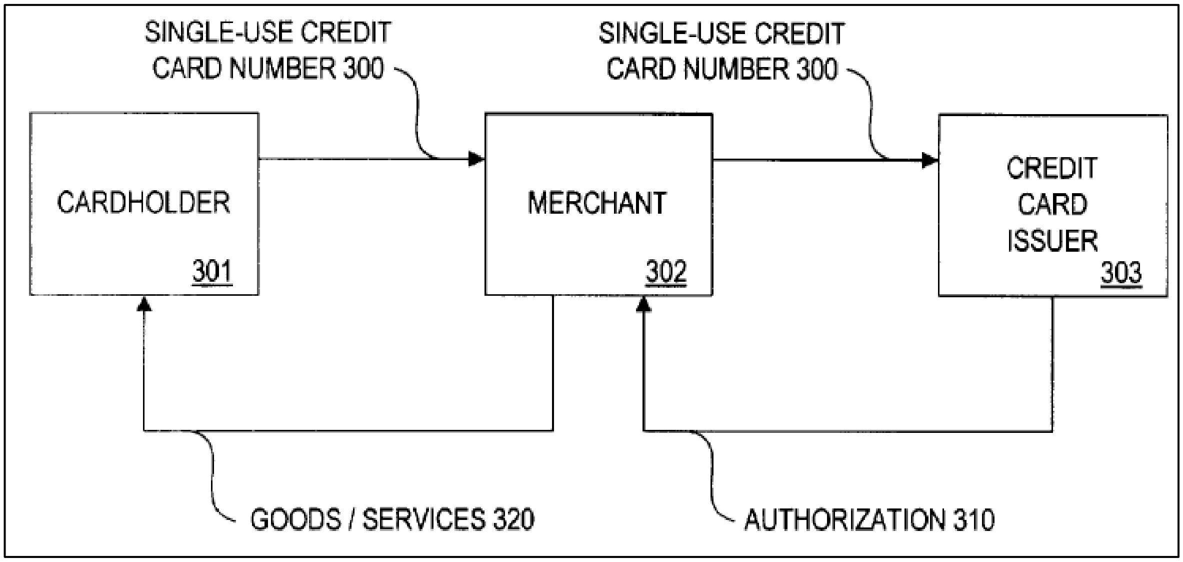


FIG. 2B

Id., Fig. 2B (POS device 200, in communication with host 300).

2. Overview of Walker

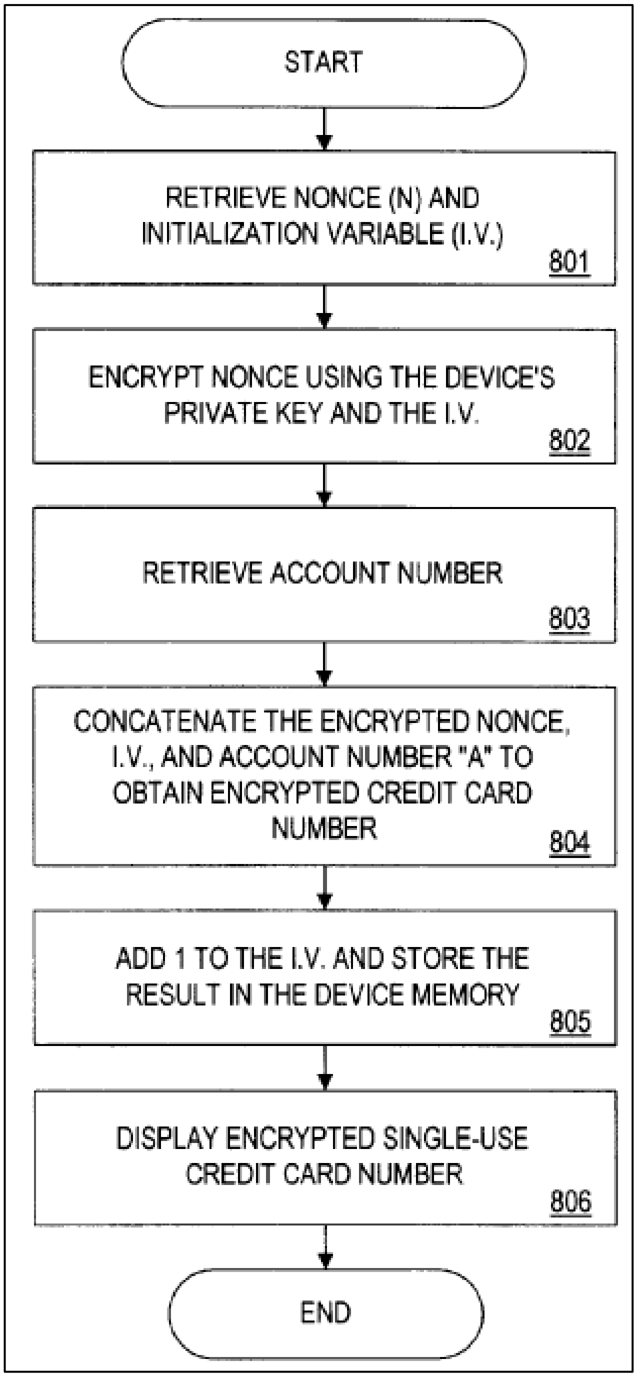
Walker (EX1012) was filed Aug. 28, 1997 and issued December 19, 2000; thus, Walker is prior art under at least §§ 102(a) and (e), as well as § 102(b) if the effective filing date of the ’181 Patent is later than December 19, 2001. *See* Sec. II.B, *supra*. Walker describes a device for use in financial transactions that includes a cryptographic processor. *Walker* (EX1012), Abstract; *see also* Figs. 1-2. The processor uses a cryptographic key to encrypt at least two data elements to generate a single-use financial identifier, such as a single-use credit card number that, from the perspective of an outside, would appear to be a conventional credit card or account number. *Id.*; *see also* 5:49-52, 6:35-37; *see also* 6:54-59, 6:66-7:3 (distinguishing the single use "credit card number" from an unchanging account number assigned to the particular cardholder). The device communicates the encrypted information to a point-of-sale terminal, which in turn sends this data, either directly or indirectly, to an issuer's central processor for validation of the cardholder and authorization of the transaction:



Id., Fig. 3A; *see also* Fig. 3B.

In one embodiment, the data elements used to generate the single-use number include a nonce N associated with the account number, an initialization variable IV that is stored in the device memory and incremented with each generation of a single-use number, and part of the user's account number. *Id.*, 7:31-51; *see also* Figs. 6-7.

The card encrypts the nonce N using the initialization variable IV and a private key, which is also stored at a central database associated with an issuer. *Id.*, 8:9-19, Fig. 8; *see also* 7:29-36, Fig. 6 (describing the central issuer database). The resulting value (C) is concatenated with the user's initialization variable IV and the unchanging account number A to create the single-use credit card number CCN. *Id.*, 8:20-25. The initialization variable IV is incremented by one, and the resulting CCN is read, shown, or transmitted to a merchant. *Id*. 8:27-35. This process is depicted in Figure 8:


START
RETRIEVE NONCE (N) AND INITIALIZATION VARIABLE (I.V.)
801
ENCRYPT NONCE USING THE DEVICE'S PRIVATE KEY AND THE I.V.
802
RETRIEVE ACCOUNT NUMBER
803
CONCATENATE THE ENCRYPTED NONCE, I.V., AND ACCOUNT NUMBER "A" TO OBTAIN ENCRYPTED CREDIT CARD NUMBER
804
ADD 1 TO THE I.V. AND STORE THE RESULT IN THE DEVICE MEMORY
805
DISPLAY ENCRYPTED SINGLE-USE CREDIT CARD NUMBER
806
END

Id., Fig. 8.

The issuer extracts the account number, the IV, and the encrypted nonce from the single-use credit card number and then (1) determines whether the account number is a valid account, (2) determines whether the initialization value recorded in the database, and (3) decrypts the encrypted nonce using the private key and compares the result with the nonce stored in the database.

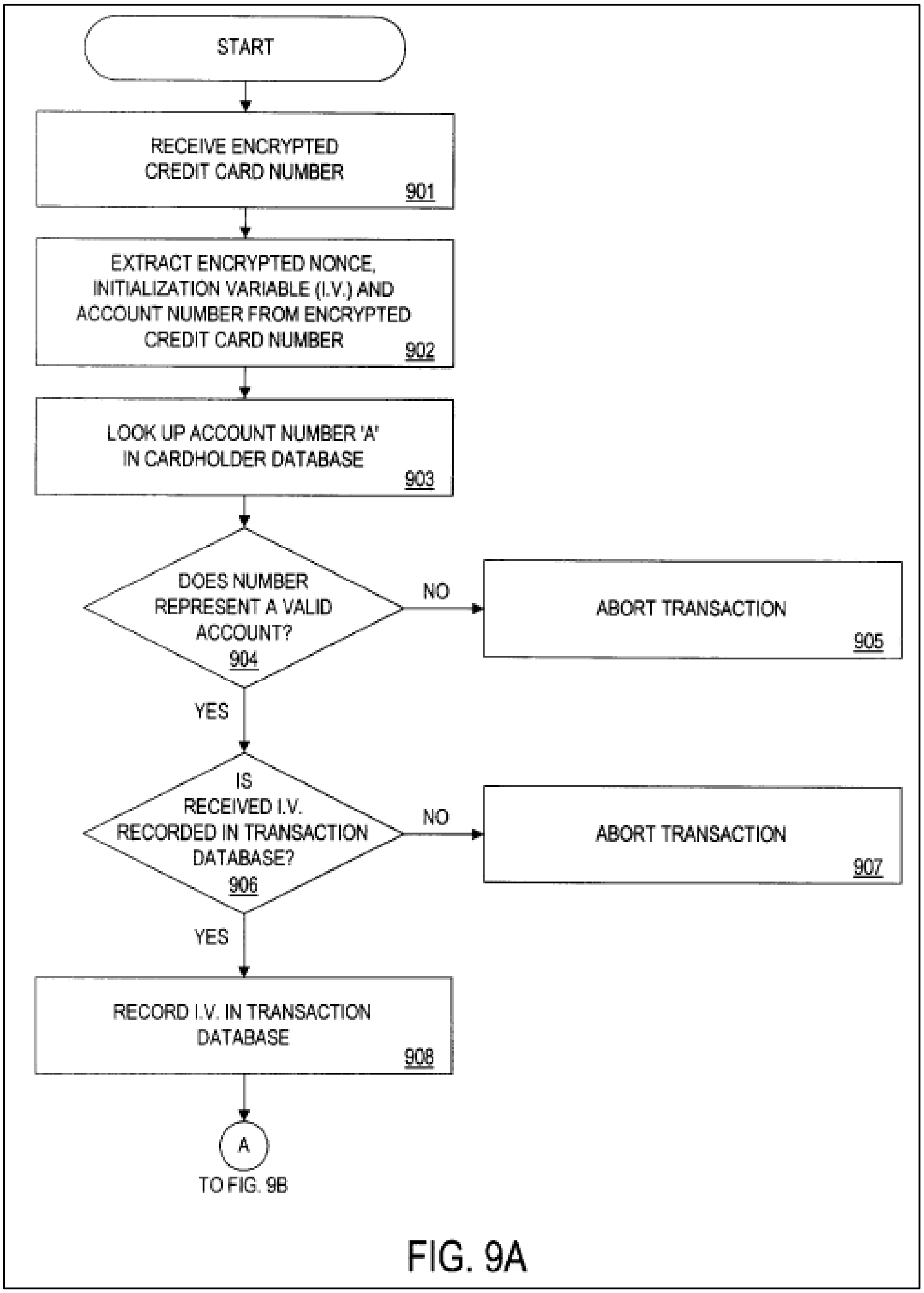

START
RECEIVE ENCRYPTED CREDIT CARD NUMBER
901
EXTRACT ENCRYPTED NONCE, INITIALIZATION VARIABLE (I.V.) AND ACCOUNT NUMBER FROM ENCRYPTED CREDIT CARD NUMBER
902
LOOK UP ACCOUNT NUMBER 'A' IN CARDHOLDER DATABASE
903
DOES NUMBER REPRESENT A VALID ACCOUNT?
904
NO
ABORT TRANSACTION
905
YES
IS RECEIVED I.V. RECORDED IN TRANSACTION DATABASE?
906
NO
ABORT TRANSACTION
907
YES
RECORD I.V. IN TRANSACTION DATABASE
908
A
TO FIG. 9B

FIG. 9A

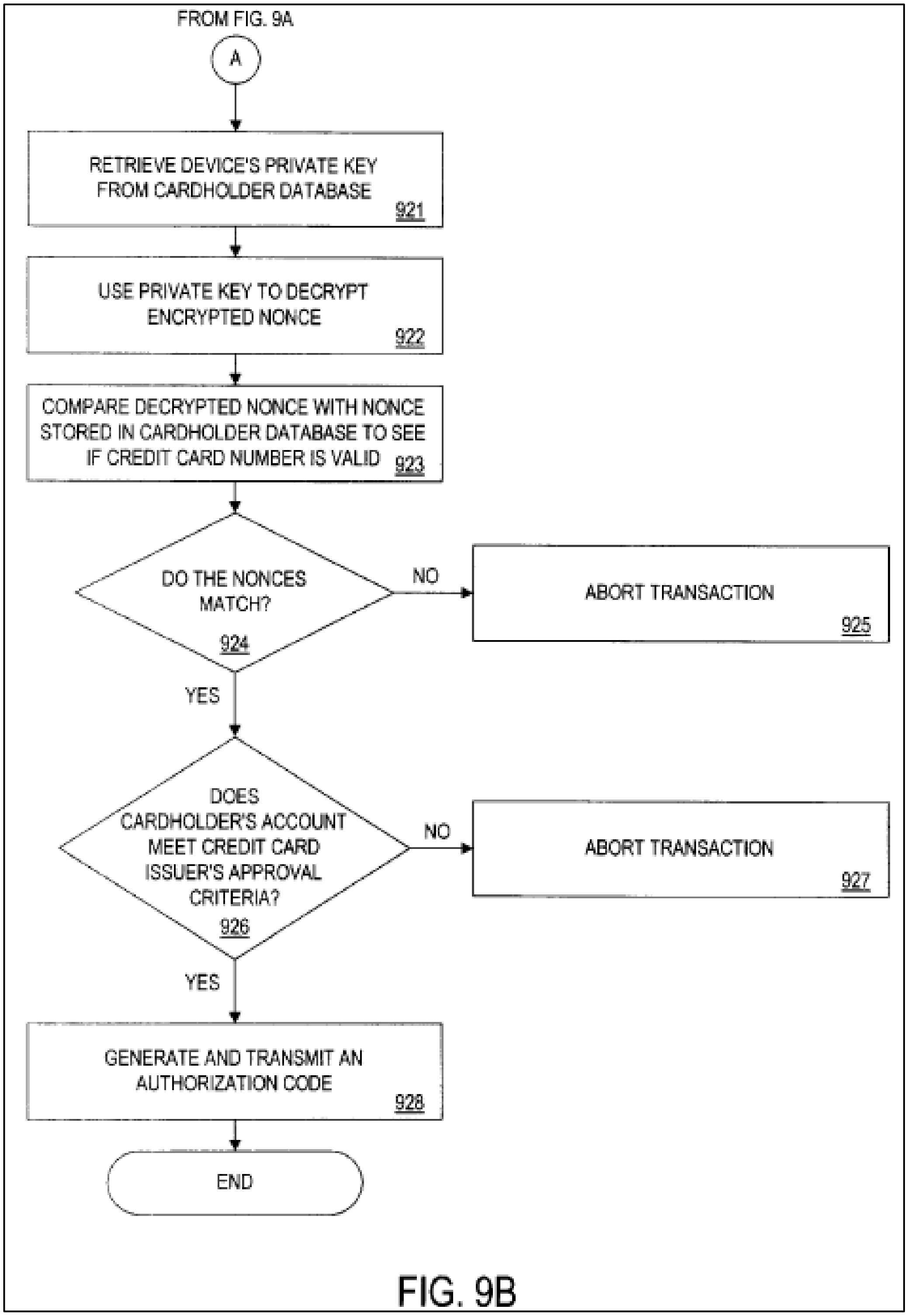

FROM FIG. 9A
A
RETRIEVE DEVICE'S PRIVATE KEY FROM CARDHOLDER DATABASE
921
USE PRIVATE KEY TO DECRYPT ENCRYPTED NONCE
922
COMPARE DECRYPTED NONCE WITH NONCE STORED IN CARDHOLDER DATABASE TO SEE IF CREDIT CARD NUMBER IS VALID
923
DO THE NONCES MATCH?
924
NO
ABORT TRANSACTION
925
YES
DOES CARDHOLDER'S ACCOUNT MEET CREDIT CARD ISSUER'S APPROVAL CRITERIA?
926
NO
ABORT TRANSACTION
927
YES
GENERATE AND TRANSMIT AN AUTHORIZATION CODE
928
END

FIG. 9B

Id., Figs. 9A-9B; *see also*, 8:40-9:3.

Walker is analogous art to the ’181 Patent. Walker is within the field of endeavor of the '181 Patent because it relates to secure financial transactions. *Id.*, Abstract; *see also* 3:59-64; *see also McNair Decl.* (EX1015), ¶70. Additionally, Walker is reasonably pertinent to at least one problem concerning the inventor of the '181 Patent: preventing theft of a user's account information, such as their account number. *Walker* (EX1012), 2:43-53. *McNair Decl.* (EX1015), ¶70.

3. Claim 1

[1P]. A method comprising:

To the extent the preamble is limiting, both Johnson and Walker disclose methods. *Johnson* (EX1011), Abstract, claim 60; *see also* 4:5-6; *see also Walker* (EX1012), 1:6-10.

[1.1]. generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader;

As mentioned in Section II.A.2, claim 1 recites a method from the perspective of an RFID device, wherein the device generates **an authentication tag** using three elements: (1) a **random number** received from an RFID reader, (2) a **transaction device identifier**, and (3) a **counter value**.

This limitation is obvious over Johnson in view of Walker. When modified in light of Walker's teachings, Johnson's system would use an encryption technique that incorporates the use of a counter value (e.g., Johnson's current sequence number as a tally of transactions) to encrypt a challenge random number received from a point-of-sale device and concatenate the result with a tag ID to generate a short code for authentication by a host. Specifically, as modified in light of Walker's disclosure, Johnson discloses *generating, in a radio frequency identification (RFID) transaction device* (e.g., tag/transponder 100)[15], *an RFID transaction device authentication tag* (e.g., an **encrypted random number ECRN**, concatenated with a tag ID) *using a random number* (e.g., the **original random number** received from the POS device, or **CRN**), *a transaction device identifier* (e.g., as modified by Walker, the encrypted random number is concatenated with a **tag ID**), *and a counter value* (e.g., as modified by Walker, the CRN is encrypted using both a main tag key and **the current sequence number** tracked in Johnson's tag/transponder, which is an analogue to Walker's initialization variable) *wherein the random number is received from an RFID reade*r (e.g., the CRN is received from the point-of-sale, or POS,

[15] As discussed in the overview of Johnson, a POSA would have appreciated that tag/transponder 100 and POS terminal 200 are RFID devices based on Johnson's use of terms of art related to RFID technology, or, at the very least, that it would have been obvious to implement them as such in light of Johnson's disclosure and a POSA's general knowledge and skill about RFID technology at the time of the invention. *See* Sec. IV.B.1, *supra*; *see also McNair Decl.*, ¶¶65, 39.

device).

As is relevant to this limitation, Johnson discloses that POS device "generate[s] and send[s] **a random number (CRN)** to the tag 100," as authentication check data; the tag then "encrypts the random number and returns the **encrypted random number (ECRN)**[16] to the POS device 200 **along with a tag identification number (ID)**." *Id.*, 10:16-22; *see also* 3:29-34 ("The POS device will generate authentication check data, preferably a random number, and send it to the tag for encryption. The tag then encrypts the random number with an encryption technique using a main cryptography key and transmits the encrypted random number back to the POS device.); 3:54-56 ("The tag random number is preferably

[16] In at least one example in the main embodiment, Johnson refers to this value as a tag random number, or TRN. *Johnson* (EX1011), 10:16-22. However, Johnson uses the "TRN" acronym in later embodiments to refer to a random number generated by the tag in order to create a session key for a different purpose. *See, e.g., id.*, 13:4-42. While the proposed combination does not exclude the practice of these additional techniques, they are not directly relevant to the mapping of the claimed authentication tag. Therefore, when referring to the encrypted random number, Petitioner uses the ECRN acronym, with the caveat that Johnson also uses the acronym TRN to refer to this concept in its specification. *See, e.g., id.*, 10:16-22.

generated upon receipt of the random number generated at the POS device."); *see also* 3:60-64; 10:54-59, 11:11-21, 13:8-16, 13:60-65, 15:41-16:5; 22:27-42 (describing different, but related, embodiments of the encryption methods used). The POS device forwards the encrypted random number ECRN the tag ID, and the original random number CRN to a host 300, which is the issuing entity that maintains the account and financial information associated with the tag. *Id*., 10:22-25; *see also, e.g.*, 3:34-38, 10:59-62 (similar disclosures); *see also* 3:11-15, 9:26-37.

Johnson's host uses the tag ID to recalculate or look up the main tag key and performs either encryption on the CRN (resulting in an "NERN") or decryption on the TRN, compares the result with the TRN or CRN, respectively, and determines whether the numbers match. *Id*., 10:34-41; *see also* 3:36-44, 10:63-11:6 (similar disclosures); *see also* 11:6-8 (alternatively, host may decrypt an encrypted random number) *see also* 8:55-65, 9:62-10:8 (describing the generation of the tag ID and main tag key). Figure 5 illustrates the communication of these elements (the CRN, ECRN, and tag ID) between the different components of the transaction system:

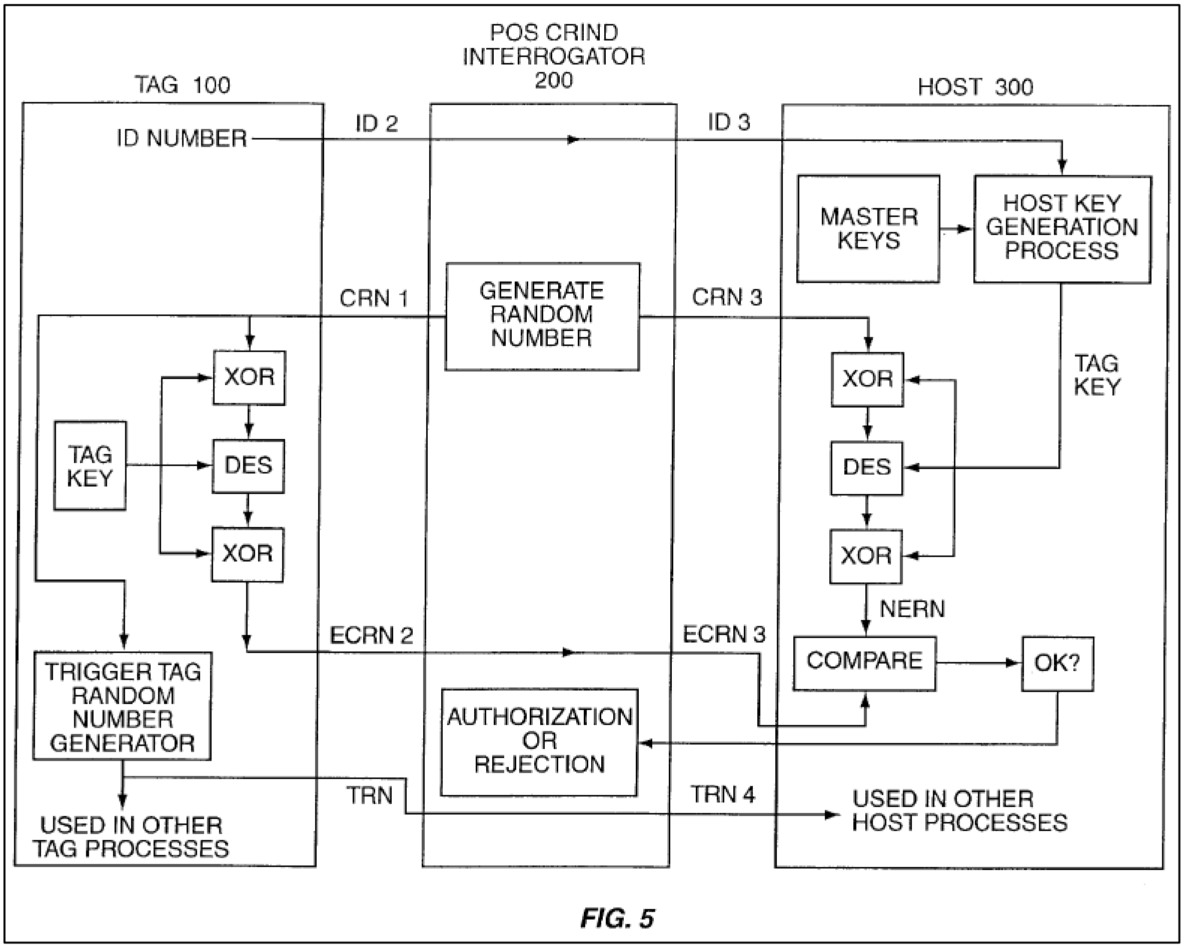

POS CRIND INTERROGATOR 200
TAG 100
HOST 300
ID NUMBER
ID 2
ID 3
MASTER KEYS
HOST KEY GENERATION PROCESS
CRN 1
GENERATE RANDOM NUMBER
CRN 3
XOR
TAG KEY
DES
XOR
XOR
DES
XOR
NERN
ECRN 2
ECRN 3
COMPARE
OK?
TRIGGER TAG RANDOM NUMBER GENERATOR
AUTHORIZATION OR REJECTION
TRN
TRN 4
USED IN OTHER HOST PROCESSES
USED IN OTHER TAG PROCESSES

FIG. 5

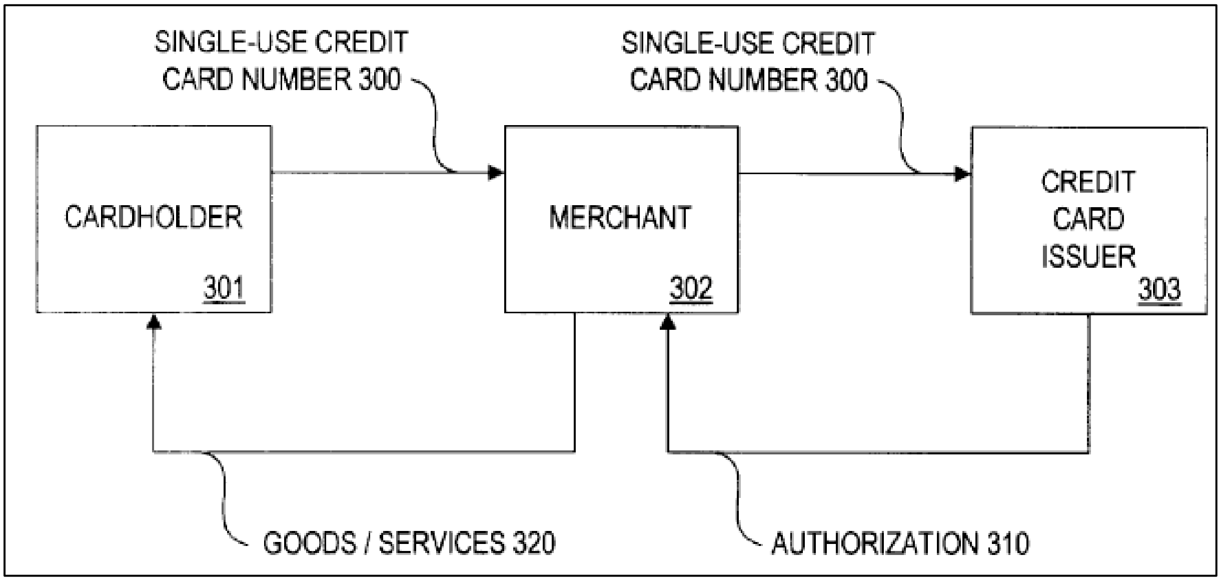
Id., Fig. 5; *see also* Figs. 1, 2A-2C (illustrating the different system components).

Johnson also discloses that the tag memory keeps track of a "**current sequence number**," which "preferably corresponds to **a tally of transactions**." *See id*., 11:52-54; *see also* 11:10-16.[17] The current sequence number is communicated

[17] The current sequence number should not be confused with the individual tag's sequence number used in the tag ID. *Id*., 9:31-34. Further, while Johnson discloses that the current sequence number could also represent the number of operations the

to a POS device to prevent a given command or action from accidentally being replicated. *Id*., 11:46-52. The tag may increment the sequence number upon receipt of the CRN from the POS device. *Id*., 16:54-67. This number may also be used by the host, which includes the current sequence number "with each command," so that the tag can compare the number with what it has stored to confirm that the host sent the command. *Id*., 11:54-60.

Walker discloses a similar transaction method using analogous entities: a cardholder, a merchant, and a host credit card issuer that cryptographically validates the cardholder:



Id., Fig. 3A; *see also* Figs. 1-2, 3B-3C (further illustrating the relationship and

tag has conducted and uses this example in some of its embodiments, Petitioner refers to the disclosure of the tally of transactions for the purposes of this mapping.

architecture of the transaction system components); *see also* 3:59-64, Abstract. Walker also discloses using similar pieces of information to generate a short authentication string as Johnson and the '181 Patent. Specifically, Walker discloses a method of creating an authentication tag (e.g., a **one-time credit card number CCN**), in which a cardholder's device encrypts a **nonce value** N using a private key and an **initialization variable IV**, which is increased by one for each transaction (EX1012, 8:27-30), and then concatenating this result, C, with the user's **account number A**, and then forwarding the result CCN to a merchant. *Walker* (EX1012), 8:9-33; *see also* 7:28-62 (describing each of the variables and the resulting credit-card number); Figs. 6-8. The merchant forwards the result to the issuer's central processor. *Id.*, 8:33-9:39. The issuer extracts C, IV, and A from the received one-time credit card number CCN, and first authenticates A and IV by comparing the values to those stored in its database. *Id.*, 8:40-54; *see also* Fig. 9A. If those values appear to be valid, the issuer looks up cardholder's private key and uses this value along with the received IV to decrypt C using the cardholder's private key and the received IV to determine if the result matches the cardholder's assigned nonce value. *Id.*, 8:55-9:3; *see also* Fig. 9B.

As combined with Walker, Johnson's tag would generate the **ECRN** (i.e., an *authentication tag*) by encrypting the **challenge random number CRN** received from the point-of sale terminal (i.e., *a random number ... received from the RFID* *reader*) using the main tag key, analogous to Walker's private key, and a **current sequence number, analogous to Walker's initialization variable** (i.e., *a counter value*) and then concatenating this result with all or part of the **tag ID** (i.e., *the transaction device identifier*). *McNair Decl.* (EX1015), ¶71. A POSA would have been motivated to implement Johnson's techniques of generating its encrypted random number ECRN using Walker's encryption techniques for generating a one-time credit card number, using the random number received from the point-of-sale device as the nonce (instead of a fixed number assigned by an issuing entity) for three reasons. *McNair Decl.* (EX1015), ¶71

First, Walker provides express motivation to incorporate its technique of including a counter value, such as its initialization variable, in the encryption process by ensuring that each credit card number is unique to a given transaction, thus preventing a "replay attack." *Walker* (EX1012), 40:37-45; *see also McNair Decl.* (EX1015), ¶¶72, 44-45.

Second, a POSA would have recognized that Walker's technique using a variable value like the initialization variable IV, analogous to Johnson's current sequence number, in the encryption process would have had the added security benefit by including a variable value known to the user and the issuer as an added check of the validity of the transaction. Specifically, by including a value that changes in a predictable manner (e.g., incrementing by one) in the encryption method, a potential hacker would not be able to commit fraud for long even if they obtained the user's key and tag ID/account number, because eventually the issuer would notice an inconsistency in the counter value from what would be expected. *See McNair Decl.* (EX1015), ¶73; *see also* ¶¶44-46 (describing how fraud is detected when counter values are used, noting that a similar rationale drove numbering checks long before encryption technologies). Thus, the proposed combination would have been a matter of using of a known technique (Walker's encryption & concatenation techniques) to improve similar methods (Johnson's encryption using a main key on a received random number) in the same way (i.e., to protect a user's account from replay attacks and by providing further validation of the token's identity). *Id.*, ¶73.

Third, the proposed combination involves merely a simple substitution of one known element (Walker's method of encrypting a number using an initialization variable, which is a counter value like Johnson's current sequence number, and concatenating the result with a tag-ID to create a one-time credit-card number) for another (Johnson's encryption of a challenge random number) to obtain predictable results (the encryption of a challenge random number with a current sequence number, and concatenating the result with a device identifier, such as a tag ID or account number). *Id.*, ¶74.

Further, a POSA would have a reasonable expectation of success in making the above proposed modifications to Johnson's methods. Johnson itself provides that the "combination of cryptography and logical operations may be ... modified" without straying from the ambit of its invention. *Johnson* (EX1011), 22:46-48; *see also* 8:10-14 (expressing preference for DES encryption but noting that "other cryptography methods are available and will work with the current invention"). Both Johnson and Walker disclose similar systems with similar goals, and no new information or hardware would be necessary to implement the encryption techniques described by Walker's disclosure into Johnson's system; for example, Johnson already discloses tracking a current sequence number that may represent a tally of transactions and that the host maintains this number for sending commands to the tag. *See, e.g.*, *id.*, 11:47-56. Therefore, a POSA would have expected the combination to require only minor modifications in software that would have yielded predictable results. *McNair Decl.* (EX1015), ¶75. Further, because the POS device in Johnson forwards both the unencrypted challenge random number and the tag ID to the issuer, all of the necessary variables for decryption would still be in the issuer's possession, and therefore, a POSA would expect the resulting operation to enable Johnson's issuer to authorize a user without compromising their information. *Id.*, ¶76. Therefore, the use of the CRN instead of the constant nonce value would not prevent the host 300 from validating either the CRN or the ECRN by replicating or reversing the encryption steps taken by the tag. *Id.*

[1.2] transmitting the RFID transaction device authentication tag to the RFID reader; and

Johnson discloses *transmitting the RFID transaction device authentication tag* (e.g., the ECRN, modified by Walker's disclosure as discussed in [1.1] above) to the RFID reader (e.g., to the POS device). *Johnson* (EX1011), 10:15-25 ("… The tag 100 encrypts the random number and returns the encrypted random number (TRN) to the POS device 200 along with a tag identification number (ID) in step 2. …"); *see also* 3:31-33, 10:56-59, Fig. 5. As modified by Walker, the generation of the encrypted random number would include the use of a counter value, such as the current sequence number as a tally of transactions, and concatenation with a tag ID. *See* [1.1], *supra*. Notably, Walker also discloses transmitting the analogous one-time credit card number to a merchant device. *Walker* (EX1012), 8:31-35, Fig. 8.

[1.3] incrementing the counter value;

Johnson in view of Walker renders this limitation obvious. Johnson explains that the "current sequence number preferably **corresponds to a tally of transactions** or operations the tag has conducted," and "increment[s] sequence number" as part of a reply to receiving the CRN from the point-of-sale device. *Johnson* (EX1011), 11:49-54, 15:54-67. Similarly, Walker discloses incrementing its initialization variable, which is analogous to the current sequence value, by one. *Walker* (EX1012), 8:27-30; *see also McNair Decl.* (EX1015), ¶71.

[1.4] wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

Johnson, as modified by Walker, discloses *an RFID transaction is authorized* (e.g., a host 300 authorizes a transaction) *in response to verification of the RFID transaction device authentication tag*. For example, Johnson discloses that a host entity host uses information associated with the tag ID number received from the POS terminal to encrypt the CRN and compare its result to the tag's encrypted random number forwarded by the terminal—if they match, the host determines that the tag is valid and authorized. Alternatively, the host may decrypt the encrypted random number using the information associated the tag ID and compare it to the tag's random number (and, as modified by Walker, the current sequence number):

> The host 300 calculates the main tag key from the ID number in the same manner in which the host 300 originally generated the main tag key (see FIG. 4). The random number (CRN) originally generated by the POS device 200 is encrypted by the host 300 to provide a host network encrypted random number (NERN). The host 300 then compares the encrypted random number (ECRN) encrypted at the tag 100 to the host network encrypted random number (NERN). **If the ECRN and NERN match, then the host signals the POS device 200 or site controller 28 that the tag 100 is valid and authorized. Alternatively, the host 300 may decrypt the encrypted random number (ECRN) and compare the result to the random number (CRN)**.

Johnson (EX1011), 10:63-11:8; *see also* 3:11-21, 3:34-44, 10:27-41, 14:6-15.

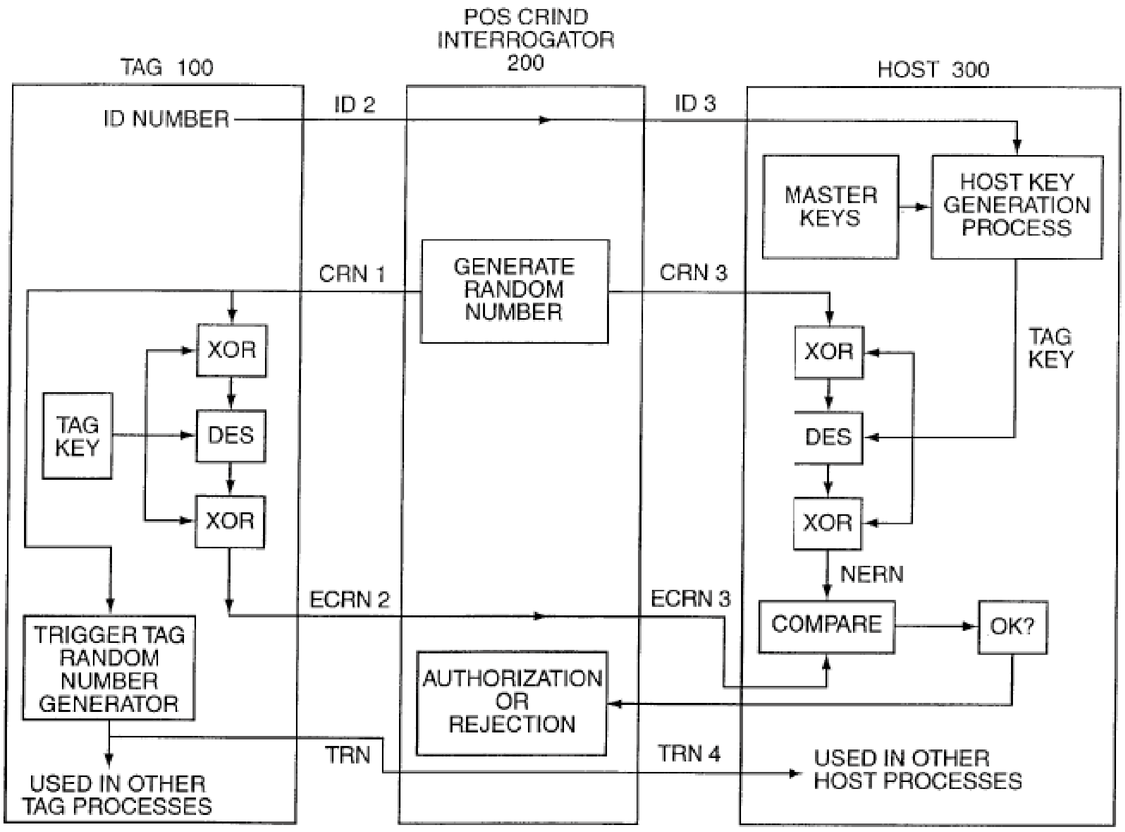


FIG. 5

Id., Fig. 5. Similarly, Walker discloses that a transaction is authorized in response to an issuer's verification of a one-time credit card number CCN. *See* [1.1], *supra*.

4. Claim 2

2. The method of claim 1, further comprising transmitting unencrypted data, the counter value, and the random number to the RFID reader.

As discussed in Sec. IV.B.3, Claim 1 is obvious over Johnson in view of Walker. Further, Claim 2 is obvious over Johnson in view of Walker.

Johnson discloses transmitting unencrypted data, such as the tag ID, to the POS device to begin a transaction. *Johnson* (EX1011), 10:19-22; *see also* 3:15-18, 10:53-56.

Additionally, Johnson discloses sending the current sequence number to the POS device (i.e., RFID reader) so that the POS device may "prevent a command or operation from accidentally being replicated." *Id.*, 11:47-52.

Finally, Johnson discloses sending the ECRN (i.e., *the random number*) to the POS device (i.e., RFID reader) in encrypted form. *Johnson* (EX1011), 10:19-22; *see also, e.g.*, 15:41-51, 16:1-2. Because in the proposed combination, Johnson's host would reconstruct the original CRN or decrypt the ECRN to recover the CRN, a POSA would have appreciated that the ECRN is the CRN (i.e., the *random number*) that is transmitted, but in encrypted form. *McNair Decl.* (EX1015), ¶76.

5. Claim 4

4. The method of claim 1, wherein the counter value is incremented a predetermined amount.

Claim 4 is obvious over Johnson in view of Walker. As discussed regarding limitation 1.3, both Johnson and Walker teach incrementing analogous *counter values*, e.g., the current sequence number and initialization variable, respectively.

Johnson explains that, as an example, the current sequence number may represent a "**tally of transactions**," or operations. *Johnson* (EX1011), 11:49-54.

Further, throughout its disclosure, whenever it describes this value being incremented as a number of operations, it discloses incrementing the value by one (i.e., a predetermined amount). *See, e.g.*, *Johnson* (EX1011), 11:54-60; *see also McNair Decl.* (EX1015), ¶¶63 n.3, 44-46. Likewise, Walker discloses incrementing the analogous initialization variable by one (i.e., by *a predetermined amount*) for every single-use credit card number generated. *Walker* (EX1012), 8:27-30. Indeed, Petitioner's expert has explained that incrementing the counter value by some *undetermined* amount or pattern would not make much sense. *McNair Decl.* (EX1015), ¶46. Thus, the additional limitation of Claim 4 is obvious over Johnson in view of Walker.

6. Claim 6

[6P]. A method comprising:

To the extent the preamble is limiting, Johnson and Walker disclose methods. *See supra*, Sec. IV.B.3 [1.pre], *supra*.

Claim 6 describes limitations similar to those of Claim 1, but from the perspective of the RFID reader. For the same reasons discussed regarding Claim 1 and below, Claim 6 is obvious over Johnson in view of Walker.

[6.1]. generating a random number at a radio frequency identification (RFID) reader;

As discussed regarding limitation 1.1, Johnson discloses, or at least renders obvious, *generating a random number* (e.g., a CRN) *at an RFID reader* (e.g., POS terminal 200). *See* Sec. IV.B.3 [1.1], *supra*; *see also, e.g.*, *Johnson* (EX1011), 10:18-19, 10:54-56, 3:29-31, Fig. 5.

[6.2]. transmitting the random number to an RFID transaction device; and;

As discussed regarding limitation 1.1, Johnson discloses *transmitting the random number* (CRN) *to an RFID transaction device* (e.g., tag/transponder 100). *See* Sec. IV.B.3 [1.1], *supra*.

[6.3] receiving, from the RFID transaction device, an RFID transaction device authentication tag, wherein the RFID transaction device authentication tag was generated using a transaction device identifier, a counter value, and the random number.

Limitation 6.3 is similar to limitations 1.1 and 1.2, but is written from the perspective of the RFID reader. *See* Sec. IV.B.3 [1.1]-[1.2], *supra*. As discussed regarding limitations 1.1 and 1.2, this limitation is obvious over Johnson in view of Walker. Specifically, as modified by Walker, Johnson discloses *receiving, from the RFID transaction device* (e.g., tag/transponder)*, an RFID transaction device authentication tag* (e.g., the ECRN concatenated with a tag ID, optionally structured as a one-time credit card number in light of Walker's disclosure)*, wherein the RFID transaction device authentication tag was generated using a transaction device identifier* (e.g., a tag ID)*, a counter value* (e.g., a current sequence number, analogous to Walker's initialization variable)*, and the random number* (e.g., the

CRN). *See* Sec. IV.B.3 [1.1]-[1.2], *supra*.

[6.4] wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

Limitation 6.4 is identical to limitation 1.4. As discussed regarding limitation 1.4, Johnson, as modified by Walker, discloses *wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag*. *See* Sec. IV.B.3 [1.4], *supra*.

7. Claim 7

7. The method of claim 6, further comprising receiving unencrypted data, the random number, and the counter value from the RFID transaction device.

As discussed, Claim 6 is obvious over Johnson in view of Walker. Claim 7 is identical to Claim 2, except that it is written from the perspective of the reader instead of the transaction device. For the reasons discussed regarding Claim 2, to which this limitation is identical, Claim 7 is obvious over Johnson in view of Walker. *See* Sec. IV.B.4, *supra*.

C. Ground 4: Claims 1, 2, 4, 6, and 7 are obvious over Johnson, Walker, and Davis

1. Overview of Davis

Davis (EX1013) was filed June 9, 1994 and issued November 19, 1996; thus, Davis is prior art at least under 35 U.S.C. §§ 102(a), (b), and (e). Davis relates to transaction systems and methods between a card with an integrated circuit, called a "stored value card" or SVC, and a security module, such as a point-of-sale terminal or vending machine. *Davis* (EX1013), Abstract, 3:42-59; *see also* 5:16-37 (describing the types of terminals usable with the SVC.

Similar to the '181 Patent and Johnson, Davis discloses incrementing a transaction counter upon receipt of a random number from a security module. *Id.*, 13:6-11; *see also* 11:36-51 (a transaction count that begins at 0 and is incremented each time a transaction is conducted is stored in the memory of the SVC); 15:25-30 ("**Like the SVC**, the security module includes **a transaction counter which is incremented by one when a transaction is conducted** with the corresponding terminal."). Then, Davis discloses using the transaction count value to generate a session key, which is then used to encrypt the random number. *Id.*, 13:12-22.

Davis is analogous art to the '181 Patent. Davis is within the field of endeavor of the claims of the '181 Patent because it relates to secure financial transactions, and it even relates to transactions using contactless technology and authentication using a random number as well as a counter value. *Id.*, Abstract; *see also* 8:31-37, 13:6-22; *see also McNair Decl.* (EX1015), ¶79. Additionally, Davis identifies utilizing transaction systems "in a convenient and secure manner" to allow circuit cards to be used in place of cash, and a POSA would have reasonably availed itself to a disclsoure with such goals to accomplish the '181 Patent's goals of reducing transaction time and protecting a user's identifying information. *See Davis* (EX1013), 1:6-12; *see also '181 Patent* (EX1001), 2:54-3:16; *McNair Decl.*

(EX1015), ¶79.

2. Motivation to Combine Johnson, Walker, and Davis

As discussed in Ground 3, claims 1, 2, 4, 6, and 7 are obvious over Johnson in view of Walker. Further, these claims are obvious over Johnson in view of Walker and Davis.

Davis is cited for its characterization of the component that tracks the number of transactions as a "counter," as in limitations 1.1 and 6.3 and Claim 2, that is incremented by a predetermined amount for each transaction, as is applicable to limitation 1.3 and Claim 4, discussed in Section II.B. A POSA would have recognized that a counter is merely a component that counts something, usually sequentially, and although Johnson refers to this concept as a current sequence number and Walker refers to it as a "initialization variable," a POSA would have recognized that these are just different ways of referring to the same concept. *McNair Decl.* (EX1015), ¶77. However, to the extent Patent Owner attempts to draw some distinction between these concepts, a POSA would have found it obvious to use Davis's transaction counter in place of the current sequence number in Johnson's transaction system, as modified in light of Walker.

A POSA would have been motivated to use a counter value, such as a transaction count, in place of Johnson's current sequence number because such a modification would have required at most a simple substitution of one known element (a transaction counter value) for another similar element (a current sequence number that is a tally of transactions) to obtain predictable results (the incrementing of a counter to track a number of transactions). *McNair Decl.* (EX1015), ¶80. Further, a POSA would have had a reasonable expectation of success in making the proposed combination because it would have only required minor modifications to Johnson's tag software and would have not changed the fundamental operation or architecture of its transaction system, and, therefore, would have yielded predictable results. *Id.*, ¶81. Therefore, claims 1, 2, 4, 6, and 7 are obvious over Johnson in view of Walker in further view of Davis.

D. Grounds 5 and 6: Claims 1, 2, 4, 6, and 7 are obvious over Johnson, Walker, and Nerlikar (Ground 5) and Johnson, Walker, Davis, and Nerlikar (Ground 6)

1. Overview of Nerlikar

Nerlikar (EX1014) was filed July 29, 1994 and issued May 13, 1997; thus, Nerlikar is prior art at least under 35 U.S.C. §§ 102(a), (b), and (e). Nerlikar relates to security systems and methods that provide "a secure, end-to-end fully automated solution for controlling access, transmission, manipulation, and auditability of high value information comprising an RFID transponder badge 302 and an RF reader transceiver 315 which is associated with a host peripheral or a network." *Nerlikar* (EX1014), Abstract; 1:7-11. Like Johnson and Walker, Nerlikar discloses an authorization process involving three entities, but it provides greater specificity in that this three-entity authorization process is performed using RFID transponders and readers:

> **[T]he present invention comprises three segments: a user segment, an equipment or facility segment, and a multi-user or site network segment.** The user segment is comprised of individuals wishing to send and receive information such as secure documents. For the user segment, the present invention requires intelligent identification means, **preferably RFID means as stated above. The RFID means may be any device which allows positive identification of the wearer and which provides an ability to communicate with the single or multiple host/ network equipment(s) or facility segment(s)**. … In the preferred embodiment, such identification means is preferably in the form of a user **RFID badge transponder (hereinafter "RFID badge" or "RFID transponder") or security badge**. Such an "RFID transponder" is an active or passive read only or read/write transponder which operates via radio frequency means, infrared means, or other optical means at a low, high or auto-frequency.

Nerlikar (EX1014), 6:31-62; *see also* 12:45-55 (RFID device may be an ATM card); *see also* 4:14-23, 6:9-19, Figs. 1, 2, 3A-3B. The equipment/reader segment "requires an RFID reader means." *Id.*, 7:36-47, Fig. 3C.

Additionally, like the '181 Patent, Johnson, and Walker, Nerlikar discloses that the RFID device includes an encryption device, such as an integrated circuit, to encrypt its output data. *Id.*, 4:56-65. Such encrypted data includes information like an authorized user's ID. *Id.*, 8:36-45; *see also* Fig. 4 (depicting a typical transaction request).

Nerlikar is analogous art to the '181 Patent. Nerlikar is within the field of endeavor of the '181 Patent because it discloses the use of RFID technology, including in financial transactions. *Id.*, 12:42-52; *see also McNair Decl.* (EX1015), ¶85. Additionally, Nerlikar is reasonably pertinent to at least one problem concerning the inventor of the '181 Patent, namely, the need for less time-consuming transaction processes. *See, e.g.*, *Nerlikar* (EX1014), 13:2-17 (describing the use of internal power to allow the read/write processes of an RFID transponder to function faster). Additionally, Nerlikar also discloses the use of encrypting identifying information stored on the RFID transponder in order to defeat attempts of unauthorized use of the tag's information. *Nerlikar* (EX1014), 8:36-45. Given these similar goals, a POSA interested in the solving the problems identified by the applicants of the '181 Patent would have reasonably availed himself to Nerlikar's disclosure. *McNair Decl.* (EX1015), ¶85.

1. Motivation to Combine Johnson (as modified by Walker or Walker and Davis) and Nerlikar

As discussed in Grounds 3 and 4, the Challenged Claims are obvious over Johnson in view of Walker and Johnson in view of Walker and Davis, respectively. Further, Claims 1, 2, 4, 6, and 7 are obvious over Johnson in view of Walker and

Nerlikar and Johnson in view of Walker, Davis and Nerlikar. Combined with Nerlikar, Johnson's system (as modified by Walker and Davis) would employ RFID technology in both the tag 100 and POS device 200, as recited in Claims 1 and 6. *McNair Decl.* (EX1015), ¶86.

As mentioned above, Johnson uses language consistent with RFID terminology, such as "tag" and "interrogator," which a POSA would have appreciated are terms of art commonly used in referring to components of RFID systems. *Id*. However, to the extent this is not sufficient to disclose the claimed RFID device and RFID reader, Nerlikar confirms the use of RFID tags and readers, including tags capable of encrypting data, and explains that such were applicable in the context of banking transactions. *Id*. In light of Nerlikar's teachings, a POSA would have found it obvious to implement Johnson's tag and POS terminal as an RFID transaction device and RFID reader, respectively. *Id*.

A POSA would have been motivated to make the combination for two reasons. First, Nerlikar provides express motivation to combine, as it discloses that such systems (including its own invention) are user-customizable and applicable to "broad application domains." *Nerlikar* (EX1014), 3:57-62. Indeed, Nerlikar specifically recognizes the application of its RFID authentication system to commercial applications, such as with ATMs and POS terminals in the retail world. *See id*., 12:45-55; *McNair Decl.* (EX1015), ¶87. Second, implementing Johnson's tag/transponder and POS device using RFID technology would have been a simple matter of using a known technique (RFID technology) to improve similar systems (Johnson's secure transaction system) in the same way, as the use of RFID technology was known to provide a secure and convenient means of communicating data. *McNair Decl.* (EX1015), ¶87.

Further, a POSA would have had a reasonable expectation of success in implementing Johnson's system using RFID components, as disclosed by Nerlikar, as a Nerlikar shows that RFID devices were highly capable of being implemented as part of a three-segment system, like Johnson's, and encrypting data using random numbers. *Id.*, ¶88; *see also Nerlikar* (EX1014), 6:31-62, Figs. 1, 2, 3A-3B. Additionally, a POSA would have known that RFID devices were increasingly being used in various contexts, including financial transactions, further increasing their expectation of success. *McNair Decl.* (EX1015) Thus, Claims 1, 2, 4, 6, and 7 are obvious over Johnson in view of Walker and Nerlikar (Ground 5) and over Johnson in view of Nerlikar and Davis (Ground 6).

V. DISCRETIONARY CONSIDERATIONS

A. Denial under § 325(d) is unwarranted

The Petition should not be rejected under 35 U.S.C. § 325(d) because it includes at least one ground set that cites new, noncumulative prior art and, as to the other ground set, the Office appears to have materially erred in not considering a strong prior art reference. Under §325(d), the Board uses a two-part framework: (1) first, it identifies whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims. *Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GMBH*, IPR2019-01469, Paper 6, 8-9 (PTAB Feb. 13, 2020).

As discussed in Section II.C, no office actions were entered during prosecution; however, the examiner did provide reasons for allowance, finding that the only concept not disclosed in the prior art was "the inclusion of the counter as part of the response." *'181 File History* (EX1002), 372, Notably, each of the grounds herein cite art that goes directly to this concept. And the grounds are supported by expert testimony that explains that the use of counters in validating financial transactions was a decades-old concept by the time of the '181 Patent. Therefore, the grounds herein demonstrate that, even if there is some overlap in art and arguments presented in the Office, the arguments presented herein are new enough to merit consideration, and failure to consider these references was material error relevant to the patentability of the claims.

Regarding the Wankmueller grounds, denial under § 325(d) would be inappropriate because it is not clear that the arguments related to priority were ever presented, and even if the Office had considered Wankmueller to be prior art, the examiner's failure to reject the claims over Wankmueller was an error material to the patentability of the Challenged Claims. Although a corresponding domestic patent of Wankmueller is cited on the face of the '181 Patent, Wankmueller was never substantively cited in any office action or the notice of allowance during prosecution. Indeed, it is possible that the examiner never considered whether Wankmueller was truly prior art to the '181 Patent, as Petitioner has argued here. *See '181 File History* (EX1002), 371-73 (notice of allowance, no previous rejections). There is no indication in the file history that the examiner scrutinized the applicant's priority claims to its provisional applications or gave Wankmueller the benefit of its earlier-filed provisional. Further, Wankmueller discloses or renders obvious each limitation of the independent claims, including the concepts cited as the basis for allowance (i.e., using a counter to generate an authentication tag). The lack of substantive consideration of Wankmueller's express disclosure of the use of a counter in generating an authentication code was a material error that deserves additional consideration. Had Wankmueller been considered, particularly with the benefit of the technological background provided by Mr. McNair, it's likely the Challenged Claims would have been rejected.

Regarding the Johnson-Walker grounds, although Johnson was cited in an information disclosure statement ("IDS"), (1) it was never substantively cited by an examiner in an office action,[18] and (2) it was never considered in combination with Walker, which is not in the list of cited references for the '181 Patent. *Oticon Medical AB et al. v. Cochlear Ltd.*, IPR2019-00975, Paper 15, 9-20. (PTAB Oct. 16, 2019) (*precedential*) (instituted over a patent owner's § 325(d) arguments where the ground included reference not seen during prosecution). Further, Walker goes directly to the basis of allowance of the '181 Patent.[19] Therefore, even if the first

[18] The secondary references, Davis and Nerlikar, also are not cited on the face of the '181 Patent, but, like Walker, they are listed as references on parent applications to the '181 Patent. Hundreds of references are included across these different applications, which were addressed by a different examiner.

[19] That Walker was not included as a cited reference for either the '181 Patent or its direct parent, U.S. Patent 7,735,725 (EX1016) is of particular relevance because it

prong of *Advanced* were satisfied, Walker's omission from consideration during prosecution of the '181 Patent was an error that deserves reconsideration given Walker's materiality to the basis of allowance.

B. The *Fintiv* Factors weigh against denial

The Board should not deny institution of this petition under § 314. To the best of Petitioner's knowledge, which is based on publicly available information, Patent Owner has asserted the '181 Patent in one litigation in the U.S. District Court for the Western District of Texas, against Citigroup Inc. and Citigroup NA ("Citigroup Case"). Petitioner is not a party to the Citigroup case.

Regarding the first factor, "whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted," Unified is not a participant to any proceedings involving the '181 Patent, so no stays would be necessary because no litigations are pending against Unified. Further, it is speculative whether a district

is included on the face of each of the indirect continuation-in-part parents (although not marked with an asterisk to indicate that it was cited by the examiner). *See* EX1006, p.5; EX1017, p.6; EX1018, p.4; EX1004, p.3. These continuation-in-part parent applications were examined by a different examiner; therefore, there is a reasonable explanation for why Walker may have gone overlooked during prosecution of the later patents.

court would grant a stay in any proceedings involving the ’181 Patent, and it is likely a stay would be granted in any future proceedings involving the ’181 Patent that are filed after the Institution Decision. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12 (May 13, 2020); *Western Digital Corp. v. Martin Kuster*, IPR2020-01391, Paper 10 at 8-9 (Feb. 16, 2021); *Dish Network v. Broadband iTV, Inc.*, IPR2020-01280, Paper 17 at 12-14 (Jan. 21, 2021) (“*Dish*”). This factor weighs against denial, or at best is neutral.

Regarding the second factor, “proximity of the court’s trial date to the board’s projected statutory deadline for a final written decision,” Unified is not a participant in any cases involving the ’181 Patent, and no trial date is set in the only case pending involving the ’181 Patent. Further, even if this case were relevant, whether this trial will proceed at all, let alone as scheduled, is speculative at best. *See, e.g., Dish*, 17-18 (finding this factor at most weighed slightly against a stay where the trial date was scheduled three months before a final written decision in a case in which the petitioner was also the defendant in the underlying litigation). Thus, this factor favors institution and weighs against discretionary denial.

Regarding the third factor, “investment in parallel proceedings by Court and the parties,” Petitioner is not a party to any litigation involving the ’846 Patent and, therefore, has not expended resources in this litigation . Further, Unified does not have any knowledge of resources expended by the parties in any parallel district court litigation other than public information. However, based on publicly available information, it appears that this litigation is still in its early stages. It appears that no investment has been made with respect to the merits of invalidity. No claim construction hearing is not scheduled. Further, there is no guarantee that the *Markman* will constitute a significant investment. *See, e.g., Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 11 (June 16, 2020) (informative) ("*Sands II*") (two-page *Markman* order "does not demonstrate [a] high level of investment of time and resources."). Additionally, Unified did not delay filing its Petition. The Petition was filed less than four months after the Citigroup Case was filed. *See Dish* at 20-21 (instituting notwithstanding a defendant filed more than seven months after complaint). This factor strongly favors institution.

Regarding the fourth factor, "overlap between issues raised in the petition and in the parallel proceeding," Unified is unaware of any overlap between this proceeding and the Citigroup Case other than the citation to the '181 Patent in the complaint generally. Petitioner has filed this IPR due to its unique business model of deterring non-practicing entities (NPEs) from asserting patents of poor quality against strategic technologies and industries. *See, e.g., Jakel Decl.* (EX1027), ¶¶2-3. As Petitioner's perspective, goals and business model is unique, it has independently pursued invalidity grounds, prior art and claim selection without discussion, interaction, involvement, or input of any kind with any defendant. *Id.*, ¶¶4-5, 13. Petitioner is not aware of which claims are asserted by Liberty in the Citigroup Case, or what prior art is known to the parties. Petitioner is not accused of infringement. Thus, there is a high likelihood this IPR will only overlap coincidentally with issues in the Citigroup Case. This factor therefore weighs against discretionary denial.

Regarding the fifth factor, "whether the petitioner and the defendant in the parallel proceeding are the same party," Petitioner is not a defendant. This factor favors institution.

Finally, the sixth factor, "other circumstances that impact the Board's exercise of discretion, including the merits," weighs against discretionary denial and in favor of institution. The Petition speaks for itself as to its strong merit, including identifying art and supporting expert testimony that goes directly to the basis of allowance of the '181 Patent.

VI. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of Claims 1, 2, 4, 6, and 7 of U.S. Patent No. 8,066,181.

Respectfully,

Dated: October 21, 2021 By: */Michelle Aspen/*
Michelle Aspen (No. 75,665)
Roshan Mansinghani (No. 62,429)

MANDATORY NOTICES

A. Real Parties-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that Unified Patents, LLC is the real party-in-interest, and further certifies that no other party exercised control or could exercise control over Unified's participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial. In view of *Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1242-44 (Fed. Cir. 2018), Petitioner has submitted voluntary discovery in support of its certification. *See Jakel Decl*. (Ex. 1027).

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner identifies the following related proceeding(s) involving the '181 Patent:

- *Liberty Peak Ventures, LLC v. Citigroup Inc. et al.*, No. 6:21-cv-00710-ADA (W.D. Tex.).

Petitioner has not previously challenged the '181 Patent, and Petitioner is unaware of any other challenges involving the particular grounds and evidence discussed herein.

C. Lead and Back-Up Counsel

Pursuant to 37 C.F.R. § 42.8(b)(3)-(4), Petitioner identifies the following designation and service information for lead and back-up counsel. Michelle Aspen will serve as lead counsel. Roshan Mansinghani will serve as first back-up counsel. Petitioner consents to electronic service of documents. Please direct all correspondence regarding this proceeding to lead and back-up counsel at their respective email addresses listed below. 37 C.F.R. § 42.8(b)(4).

Lead Counsel	Back-Up Counsel
Michelle Aspen (Reg. No. 75,665) michelle@unifiedpatents.com Unified Patents, LLC 4445 Willard Ave, Suite 600 Chevy Chase, MD 20815 T: 559-214-3388	Roshan Mansinghani (Reg. No. 62,429) roshan@unifiedpatents.com Unified Patents, LLC 4445 Willard Ave, Suite 600 Chevy Chase, MD 20815 T: 214.953.6737

Dated: October 21, 2021

By: /*Michelle Aspen*/
Michelle Aspen (No. 75,665)

Counsel for Petitioner

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. § 42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,623 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: October 21, 2021

By: */Michelle Aspen/*
Michelle Aspen (No. 75,665)

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on October 21, 2021, a complete and entire copy of this Petition for *Inter Partes* Review, including all exhibits listed in the Appendix of Exhibits, as well as the accompanying Power of Attorney, was provided via Federal Express to the Patent Owner by serving the counsel of record for the '181 Patent as listed on PAIR:

Brundidge & Stanger, P.C.
1925 Ballenger Avenue
Ste. 560
Alexandria, VA 22314

Dated: October 21, 2021

By: */Ashley Cheung/*
Ashley Cheung
Paralegal for Petitioner