Trials@uspto.gov
Tel: 571-272-7822

Paper: 10
Entered: July 8, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INC.,
Petitioner,

v.

LEON STAMBLER,
Patent Owner.

Case CBM2015-00044
Patent 5,793,302

Before BRYAN F. MOORE, TRENTON A. WARD, and PETER P. CHEN, *Administrative Patent Judges.*

CHEN, *Administrative Patent Judge*.

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

A. Background

MasterCard International Inc. ("Petitioner") filed a corrected petition to institute a covered business method patent review of claims 51, 53, 55, and 56 (the "challenged claims") of U.S. Patent 5,793,302 (Ex. 1001, "the '302 patent") pursuant to pursuant to § 18 of the Leahy-Smith America Invents Act ("AIA"). Paper 7 ("Pet."). Leon Stambler ("Patent Owner") submitted a Preliminary Response under 37 C.F.R. § 42.207. Paper 9 ("Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 324, which provides that a covered business method patent review may not be instituted "unless . . . it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable."

The information presented in the Petition sets forth Petitioner's contentions of unpatentability of the challenged claims under 35 U.S.C. §§ 102 and/or 103 based on the following specific grounds (Pet. 16–76):

Reference[s]	**Basis**	**Claim(s) Challenged**
Davies[1]	§ 102	51, 53, and 55
Meyer[2]	§ 102	51, 53, 55, and 56
Davies and Meyer	§ 103	51, 53, 55, and 56

[1] D. W. Davies, et al., SECURITY FOR COMPUTER NETWORKS: AN INTRODUCTION TO DATA SECURITY IN TELEPROCESSING AND ELECTRONIC FUNDS TRANSFER (2d ed. 1989) (Ex. 1004) ("Davies").

[2] C. H. Meyer, et al., CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY – A GUIDE FOR THE DESIGN AND IMPLEMENTATION OF SECURE SYSTEMS (1982) (Ex. 1022) ("Meyer").

Reference[s]	Basis	Claim(s) Challenged
Davies or Meyer and Nechvatal[3]	§ 103	55
Davies, Fischer,[4] Piosenka[5]	§ 103	56

After considering the Petition and Preliminary Response, we determine that the '302 patent is a covered business method patent and that Petitioner has demonstrated that it is more likely than not that the challenged claims are unpatentable. Accordingly, we institute a covered business method patent review of claims 51, 53, 55, and 56 of the '302 patent.

B. Related Proceedings

Petitioner indicates that the '302 patent is currently the subject of a co-pending district court proceeding, styled *Stambler v. MasterCard, Inc.*, No. 0:14-cv-60830 (S.D. Fla.). Pet. 2.

Additionally, we note that the Federal Reserve Banks previously filed two petitions for *inter partes* review of the '302 patent, the first petition in *Federal Reserve Banks v. Stambler*, Case IPR2013-00341 (PTAB June 11, 2013) (Paper 3), challenging claims 7, 9, 31, 33, 34, 41–43, 45–48 and 51–56 of the '302 patent, and the second petition in *Federal Reserve Banks v. Stambler*, Case IPR2013-00409 (PTAB June 12, 2013) (Paper 1), challenging claims 9, 28–30, 32, 35–38, 44, 49–50, and 89–90 of the '302 patent. The Board granted joint motions to terminate each of these proceedings on December 11, 2013. *See* IPR2013-00341,

[3] J. Nechvatal, PUBLIC-KEY CRYPTOGRAPHY (NIST SPECIAL PUBLICATION 800-2) (April 1991) (Ex. 1005) ("Nechvatal").

[4] U.S. Patent No. 4,868,877 (Ex. 1006) ("Fischer").

[5] U.S. Patent No. 4,993,068 (Ex. 1008) ("Piosenka").

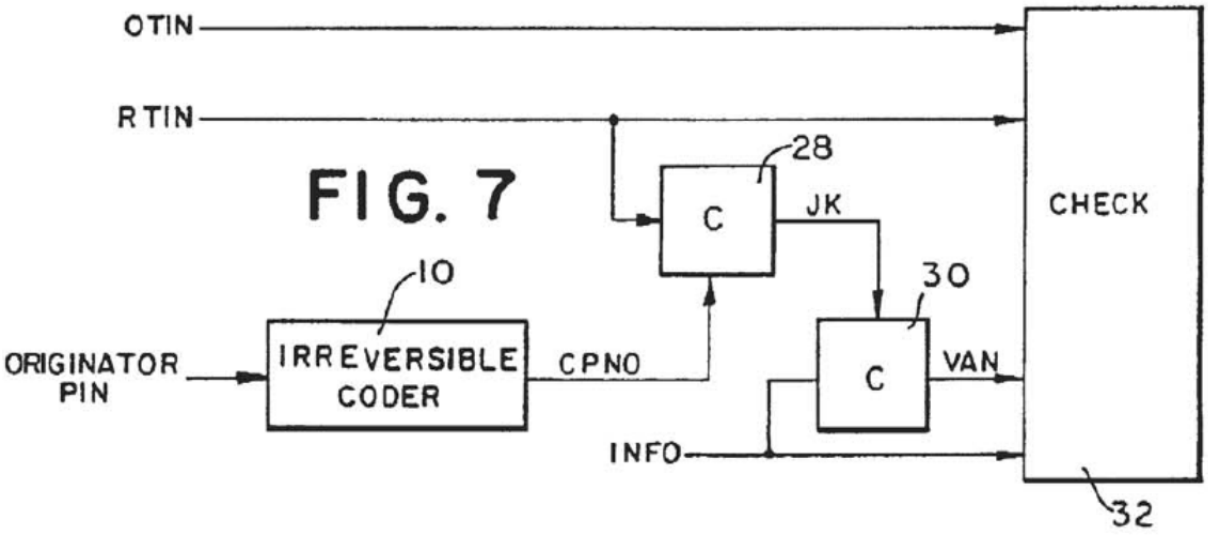
Paper 12; IPR2013-00409, Paper 11. Furthermore, on December 9, 2013, Fifth Third Bank filed a petition for *inter partes* review in *Fifth Third Bank v. Stambler*, Case IPR2014-00244 (PTAB Dec. 9, 2013) (Paper 1), challenging claims 7, 8, 31, 33, 34, 41–43, 45–48, and 51–56 of the '302 patent. On March 17, 2014, the Board granted a joint motion to terminate this proceeding. *See* IPR2014-00244, Paper 9. On April 25, 2014, Visa Inc. filed a petition for *inter partes* review in *Visa Inc. v. Stambler*, Case IPR2014-00694 (PTAB Apr. 25, 2014) (Paper 1), challenging claims 51, 53, 55, and 56. The Board denied institution. *See* IPR2014-00694, Paper 10. Finally, Petitioner herein, MasterCard International Inc., filed a petition for covered business method patent review, in *MasterCard International Inc. v Stambler*, Case CBM2015-00013 (PTAB Oct. 24, 2014) (Paper 9), challenging claims 51, 53, 55, and 56. On April 20, 2015, the Board granted a joint motion to terminate the proceeding. *See* CBM2015-00013, Paper 9.

C. The '302 Patent

The '302 patent generally relates to a transaction system for authenticating a transaction, document, or record such that the information associated with at least one of the parties involved is coded to produce a joint code. Ex. 1001, 2:7–14. Additionally, the joint code then is used to code information relevant to the transaction, document, or record to produce a Variable Authentication Number ("VAN"). *Id.* at 2:14–17. Thus, during subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to decode the VAN properly in order to re-derive the information. *Id.* at 2:20–24. The joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. *Id.* at 2:24–26. The '302 patent describes that at the time of enrolling as a user of the system, each user selects a Personal Identification

Number ("PIN"), which is secret and cannot be recovered from other information anywhere in the system. *Id.* at 2:31–36. In some embodiments described in the '302 patent, the joint code is created by requiring one participating user to provide a PIN and using the other party's non-secret identification code. *Id.* at 2:47–51.

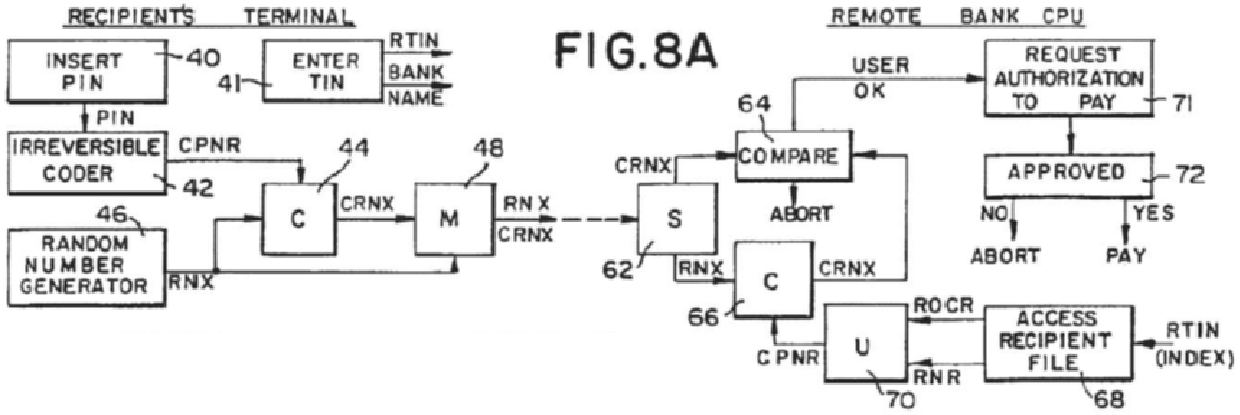
Figure 7 of the '302 patent, reproduced below, illustrates how an originator generates a check.



As shown above in Figure 7 of the '302 patent, the originator enters a PIN at a terminal, and irreversible coder 10 converts the PIN to a Coded PIN ("CPNO"), which is applied as the key input to coder 28. *Id.* at 5:3–6. The data input to coder 28 is the Recipients Taxpayer Identification Number ("RTIN"), which has been read from the check, or accessed from computer memory, or entered by the originator. *Id.* at 5:6–9. The data output of coder 28 is a joint key ("JK"), which is applied as a key input to coder 30. *Id.* at 5:9–10. The data input to coder 30 is the information ("INFO") to be authenticated, and the data output of coder 30 is the Variable Authentication Number ("VAN"). The VAN "codes the information to be authenticated, based upon information related to the recipient and information

related to the originator." *Id.* at 5:15–22. The VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction. *Id.* at 5:30–33.

Figure 8A of the '302 patent, reproduced below, illustrates the authentication process at a terminal when the recipient presents the originator's check to be cashed.



As shown in Figure 8A above, at block 40 the recipient inserts a PIN, and at block 41, the recipient identifies a bank and enters a Taxpayer Identification Number ("TIN"). *Id.* at 5:55–64. Irreversible coder 42 processes the PIN to produce the Coded PIN ("CPNR"), which is applied as the key input to coder 44. *Id.* at 5:66–6:1. A random number generator produces a random number ("RNX"), which is applied as the data input to coder 44. *Id.* at 6:1–3. Coder 44 then produces a Coded Random Number ("CRNX"), which is applied to mixer 48 along with RNX. *Id.* at 6:3–5. The mixer signal along with the information read from the check is transmitted to the computer at the recipient's bank. *Id.* at 6:12–14. At the recipient's bank, the output of mixer 48 is received at sorter 62, which separates CRNX and RNX. *Id.* at 6:22–23. Based on the RTIN, the bank's computer accesses the recipient's non-secret number and secret number, which are applied to uncoder 70 to generate the recipient's CPNR. *Id.* at 6:25–31. The

CPNR is applied as the key input to coder 66, which reproduces CRNX. *Id.* at 6:31–33. If the generated CRNX matches the received CRNX in block 64, the recipient's bank communicates with originator's bank, conveying all information regarding the transaction and requesting authorization to pay in block 71. *Id.* at 6:37–45.

Claim 51, reproduced below, is illustrative of the claimed subject matter:

> 51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, the method comprising:
>
> receiving funds transfer information, including at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount;
>
> generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;
>
> determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and
>
> transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.

Ex. 1001, 33:15–36.

D. Claim Construction

Petitioner states that the '302 patent has expired. Pet. 15. The Board's review of the claims of an expired patent is similar to that of a district court's review. *In re Rambus, Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012). The principle set

forth by the court in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1327 (Fed. Cir. 2005) (words of a claim "are generally given their ordinary and customary meaning" as understood by a person of ordinary skill in the art in question at the time of the invention, construing to preserve validity in case of ambiguity) should be applied because the expired claims are not subject to amendment.

Petitioner cites to an exhibit (Ex. 1018) reciting proposed claim constructions of certain terms in the '302 patent advanced by parties during various litigation matters involving the '302 patent and the claim constructions adopted by the Courts in those matters. *See* Pet. 16. Petitioner proposes a construction for "variable authentication number." Pet. 16. Patent Owner proposes construction for several other terms. Prelim. Resp. 6–13.

1. "variable authentication number"

In IPR2014-00694, we construed the term "variable authentication number" or "VAN" as "a variable number resulting from a coding operation that can be used in verifying the identity of a party or the integrity of information or both." Case IPR2014-00694, slip op. at 8–9 (PTAB Oct. 31, 2014) (Paper 10). Petitioner appears to argue urge for that construction to be adopted for purposes of this decision. Pet. 16. We agree with Petitioner, and adopt this construction as the broadest reasonable interpretation for purposes of this decision.

2. Sequence of method steps

Patent Owner likewise argues that we should adopt our determination from IPR2014-00694 regarding the sequence of steps recited in independent claim 51, namely, that at least a portion of the receiving step must precede the generating step. Case IPR2014-00694, slip op. at 11–14 (PTAB Oct. 31, 2014) (Paper 10). We agree with Patent Owner, and adopt this construction for purposes of this decision. We also determine that, for purposes of this decision, no explicit

construction is necessary for the other terms proposed by Patent Owner.

II. ANALYSIS

A. Covered Business Method Patent

Section 18 of the AIA provides for the creation of a transitional program for reviewing covered business method patents. A "covered business method patent" is a patent that "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). A patent need have only one claim directed to a covered business method to be eligible for review. *See* Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734, 48,736 (Aug. 14, 2012) ("CBM Rules") (Comment 8).

1. Financial Product or Service

Petitioner asserts that:

> In general, the Challenged Claims recite methods of facilitating the exchange of money from one financial account to another. Patent Owner has sued a number of financial institutions. By way of example, Challenged Claims 51, 53, 55 and 56 each recite "a method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party." There can be no question that the process of transferring funds between accounts is "financial in nature," and that authentication of such a transfer is at least "incidental to a financial activity."

Pet. 5. Patent Owner argues that the challenged "claims are directed to authenticating the parties and the instrument of the transaction." Prelim. Resp. 18. Patent Owner's argument ignores the language of the claims, including, among

other limitations, the recitations of "a method for authenticating the *transfer of funds*." Ex. 1001, claim 51 (emphasis added). We determine that the '302 patent includes at least one claim that meets the financial in nature requirement of § 18(d)(1) of the AIA.

2. Exclusion for Technological Inventions

Petitioner asserts that the challenged claims do not fall within § 18(d)(1)'s exclusion for "technological inventions." Pet. 6–10. In particular, Petitioner argues that the '302 claims do not recite a technological feature that is novel and unobvious, and do not solve a technical problem using a technical solution. *Id*. Petitioner asserts that the '302 patent recites methods of facilitating and authenticating the exchange of money from one financial account to another. Pet. 5. Petitioner states, "the '302 patent makes clear that it utilizes nothing more than conventional elements to perform its authentication task." Pet. 7. In addition, the '302 patent specifies that the asserted novelty of the invention is not in any specific improvement of software or hardware, but in the method of authenticating documents and "the individuals who are involved with them or responsible for them." Ex. 1001, 1:17–20. For example, the '302 patent states that "[t]here are many times in our daily lives when the need arises for highly secure transactions" and "a pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction" (*id.* at 1:24–25, 1:50–54).

The '302 patent further states that the "functional building blocks utilized in the preferred embodiments . . . are conventional building blocks," while acknowledging that the "[a]lthough preferred embodiments of the invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that many additions, modifications, and substitutions are possible without departing

from the scope or spirit of the invention" (*id.* at 3:29–32, 24:31–34). Thus, we determine that the claims are merely the recitation of a combination of known technologies, which indicates that it is not a patent for a technological invention. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012).

Patent Owner argues that the claims are directed toward solving the technological problem of verifying the identity and securing the interests of parties to multi-party transactions, and in particular, absent parties to a transaction. Prelim. Resp. 26–27. We are not persuaded by this argument because, as Petitioner argues, the problem being solved by the claims is a business problem—authentication of individuals and information in financial transactions. Pet. 5–10. Indeed, Patent Owner elsewhere concedes that the challenged "claims are directed to authenticating the parties and the instrument of the transaction." Prelim. Resp. 18. Thus, based on the particular facts of this proceeding, we conclude that the claims do not recite a technological invention and are eligible for a covered business method patent review.

3. Conclusion

In view of the foregoing, we conclude that the '302 patent is a covered business method patent under AIA § 18(d)(1) and is eligible for review using the transitional covered business method patent program.

B. 35 U.S.C. § 325(d)

Patent Owner argues that we should exercise our discretion to deny review of the challenged claims pursuant to 35 U.S.C. § 325(d). Prelim. Resp. 14–17. Rule 325(d) provides that in "determining whether to institute or order a proceeding under this chapter, chapter 30, or chapter 31, the Director may take into account whether, and reject the petition or request because, the same or

substantially the same prior art or arguments previously were presented to the Office." Patent Owner argues that the Petition should be denied under 35 U.S.C. § 325(d) because the "petition contains a whole section explaining how it will use the claim construction from the prior VISA IPR institution-denial decision [citation omitted] using the identical prior art presented there (plus Meyer)." Prelim. Resp. 15. Patent Owner adds that Petitioner analyzed Meyer in its invalidity contentions in the related district court proceeding (where Petitioner referred to Meyer as "Matyas," reflecting the name of the co-author of the reference). Prelim. Resp. 1, 2, 16; Ex. 1021, 1022.

We decline to exercise our discretion to reject the Petition under § 325(d), as the prior art and arguments presented by Petitioner are not substantially similar to those presented either in the petition filed by Petitioner in CBM2015-00013, or in the petition filed by a different petitioner, Visa Inc., in IPR2014-00694 (the "Visa IPR"). Specifically, Petitioner argues that the Meyer reference, asserted here but not in the Visa IPR or in Petitioner's previous petition in CBM2015-00013, teaches one or more limitations of all four of the challenged claims, under three different grounds. Pet. 35–69. In exercising our discretion, we consider all of the circumstances regarding this proceeding, including the fact that Meyer, and its accompanying arguments, were not previously asserted by MasterCard (or by Visa). In view of the circumstances of this proceeding, we do not exercise our discretion to decline review under § 325(d).

C. Proposed Anticipation by Davies

1. Overview of Davies

Davies is a textbook titled "Security for Computer Networks," and it provides an introduction to data security in teleprocessing and electronic funds transfer. Ex. 1004, 4. Chapter 10 of Davies is titled "Electronic Funds Transfer

and the Intelligent Token" and describes various electronic methods of payment. *Id.* at 282. Section 10.6 of Davies is titled "Payments by Signed Messages" and describes the implementation of an electronic cheque by using "a digital signature facility with a key registry to authenticate public keys." *Id.* at 328. Davies discloses that, to allow the content of the electronic cheque to be validated, it should contain the items shown in Figure 10.22 below (as annotated by Petitioner):

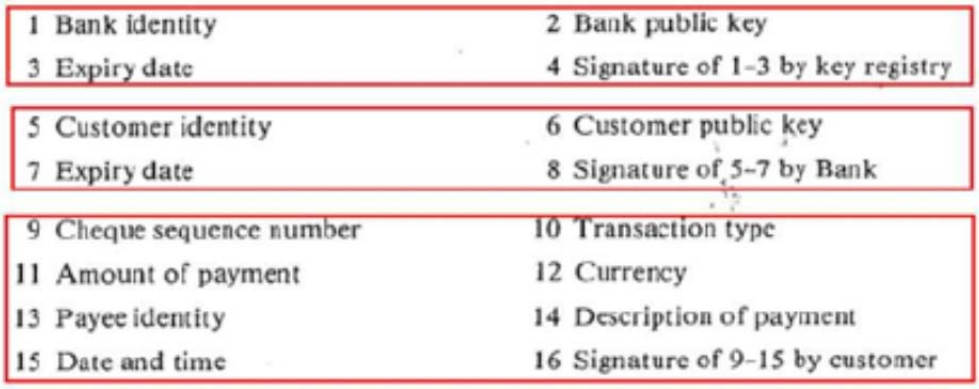


Fig. 10.22 Electronic cheque

As shown above in Figure 10.22, Davies discloses that its electronic cheque provides three sections of data. *Id.* at 328. The first is a certificate by the key registry which authenticates the bank's public key and provides an expiry date. *Id.* The second section of the electronic cheque contains the customer identity and his public key, signed by the bank and verifiable using the public key provided in the first section. *Id.* The third section provides the payment information of the cheque. *Id.* at 329. Furthermore, the "final signature by the customer, covers all the variable information in the cheque." *Id.*

Davies also discloses that private customers of the bank can carry an intelligent token or smart card to function as an electronic chequebook. *Id.* ("[f]unctioning as an electronic chequebook, the private customer's token can record the transaction[s] it makes and list them for its holders at any convenient

terminal."). Furthermore, Davies discloses that a terminal can be used to generate a cheque, sign it with the aid of the token, and send it to the beneficiary. *Id.*

In addition, Davies discloses that the "same intelligent token which provides an electronic cheque between individuals can . . . also 'cash a cheque' at an ATM with on-line verification." *Id.* at 330. Figure 10.23 of Davies is reproduced below.

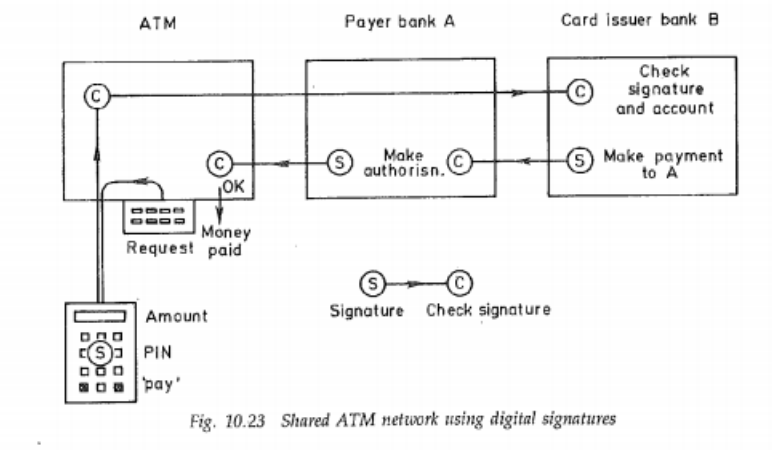


Fig. 10.23 Shared ATM network using digital signatures

Figure 10.23 illustrates a shared ATM network using digital signatures. Petitioner quotes Davies's explanation of Figure 10.23:

> Figure 10.23 shows how this works in a shared ATM network. The customer's request is formed into a message and presented to the token. Here it is signed and returned to the ATM. The ATM checks the signature to avoid passing ineffective messages into the system. If it is correct, the 'cheque' passes via the payer bank, A, to the card issuer bank, B. Here the signature is checked and the customer's account examined and. if everything is in order, debited. A payment message signed by B is sent to A. The message and its signature are checked and if all is well an authorization goes to the ATM to release the money.

Pet. 18–19; *see* Pet. 28–29; Ex. 1004, 330–31.

2. Analysis of Asserted Ground of Anticipation by Davies

Petitioner argues that claims 51, 53, and 55 are anticipated by Davies. Pet. 24–35. With respect to claim 51, Petitioner contends that Davies discloses the

transfer of funds from an account associated with a first party to an account associate with a second party. Pet. 24–25. Furthermore, Petitioner contends that Davies discloses a credential containing non-secret information by disclosing a "bank's public key" and "a certificate by the key registry which authenticates the bank's public key." Pet. 26 (citing Ex. 1004, 328). Additionally, Petitioner contends that Davies discloses the claimed "receiving funds transfer information" by disclosing that an electronic check provides the identity of the customer, the payee and the payment amount ('transfer amount')." Pet. 28 (citing Ex. 1004, 328–29, Fig. 10.22). As to the claimed step of "generating a variable authentication number (VAN) using a portion of the received funds transfer information," Petitioner cites to Davies's disclosure that the "payment information . . . forms the third section of the cheque data" and the "final signature by the customer, covers all the variable information in the cheque." Pet. 29 (citing Ex. 1004, 329). Petitioner further contends that Davies discloses that at least a portion of the receiving step precedes the generating step, citing Figure 10.23 and Davies's disclosure that "the token both receives the funds transfer information ('the customer's request is formed into a message and presented to the token') and then, after receipt of that information, the token generates a VAN using at least a portion of that received funds transfer information ('[h]ere it is signed and returned to the ATM')". Pet. 18–19, 27–29.

Finally, as to the claimed step of "transferring funds . . . if the at least a portion of the received funds transfer information and the VAN are determined to be authentic," Petitioner cites to Davies's disclosure that "the electronic cheque is transmitted . . . to the card issuer bank where the signature is checked" and the accounts of customer and merchant can be updated if the signature is verified. Pet. 33–34 (citing Ex. 1004, 330).

Patent Owner argues that Davies does not anticipate claim 51. Patent Owner first appears to assert that Davies does not disclose that a portion of the step of receiving funds transfer information precedes the step of generating a VAN. Prelim. Resp. 40. For purposes of this decision, Petitioner's evidence, namely the disclosure in Figure 10.23 and related text that "the token both receives the funds transfer information ('the customer's request is formed into a message and presented to the token') and then, after receipt of that information, the token generates a VAN using at least a portion of that received funds transfer information ('[h]ere it is signed and returned to the ATM')," adequately shows that Davies discloses receipt of funds transfer information prior to generation of a signed message. Pet. 18–19, 27–29; Ex. 1004, Fig. 10.23, 328–331. Patent owner further argues that Petitioner "mixes and matches" separate unrelated disclosures (the "cheque embodiment" and the "ATM embodiment") from Davies. Prelim. Resp. 41–43. The two "embodiments," however, are related as described by Davies, which states the "same intelligent token which provides an electronic cheque between individuals can . . . also 'cash a cheque' at an ATM with on-line verification." Ex. 1004, 330. Patent Owner makes a number of additional arguments, none of which upon review persuade us that Petitioner fails to meet its burden for purposes of this decision. Prelim. Resp. 43–50. We are persuaded that Petitioner has demonstrated that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 51 as anticipated by Davies.

For claim 53, which recites that the funds transfer comprises a payment made by the first party to the second party (Ex. 1001, 33:49–51), Petitioner describes Davies's disclosures of funds transfer from a customer to a payee using an electronic check, and also a transfer of funds from "Ann" to "Bill." Pet. 24–35. We are persuaded that Petitioner has demonstrated that it is more likely than not

that Petitioner would prevail in establishing the unpatentability of claim 53 as anticipated by Davies. With respect to claim 55, which recites that the "VAN is generated by using an error detection code" (Ex. 1001, 33:55–56), Petitioner does not argue that Davies explicitly discloses, and instead states that Davies only suggests indirectly, the recited error detection code. Pet. 69. Thus, we are not persuaded that Petitioner has demonstrated that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as anticipated by Davies.

D. Proposed Anticipation by Meyer

1. Overview of Meyer

Meyer is a textbook titled, "Cryptography: A New Dimension in Computer Data Security–A Guide for the Design and Implementation of Secure Systems," and describes encryption and authentication methods. For background, Meyer describes "a simple transaction in which cryptography is not employed," in which a customer with a personal account number with a banking institution uses a bank card and a PIN to pay a $35 grocery bill and receive $50 in cash. *Id*. at 477. Meyer generally describes techniques for applying cryptography to pin-based electronic funds transfer systems. Ex. 1022, 429–73. For example, Meyer describes using a "message authentication code" or "MAC" that is generated by using a technique "which produces cryptographic check digits which are appended to the message. . . . These digits . . . are generated by the originator, appended to the transmitted message, and then checked by the recipient, who also holds the same secret key used in the generation process." *Id*. at 457; *see also id*. at 469. If the same MAC can be generated by the recipient, then the message was not modified and the request can be approved ("[s]hould anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he

would be detected."). *Id.*

Meyer also discloses, for purposes of authenticating a transfer of funds, the use of digital signatures (DGS) based on public-key algorithms, and specifically, for example, the use of private and public key pairs, the latter of which is shared and used to authenticate transaction request messages signed by a sender with the associated private key. *Id*. at 569–76. Figure 11-44 of Meyer is reproduced below.

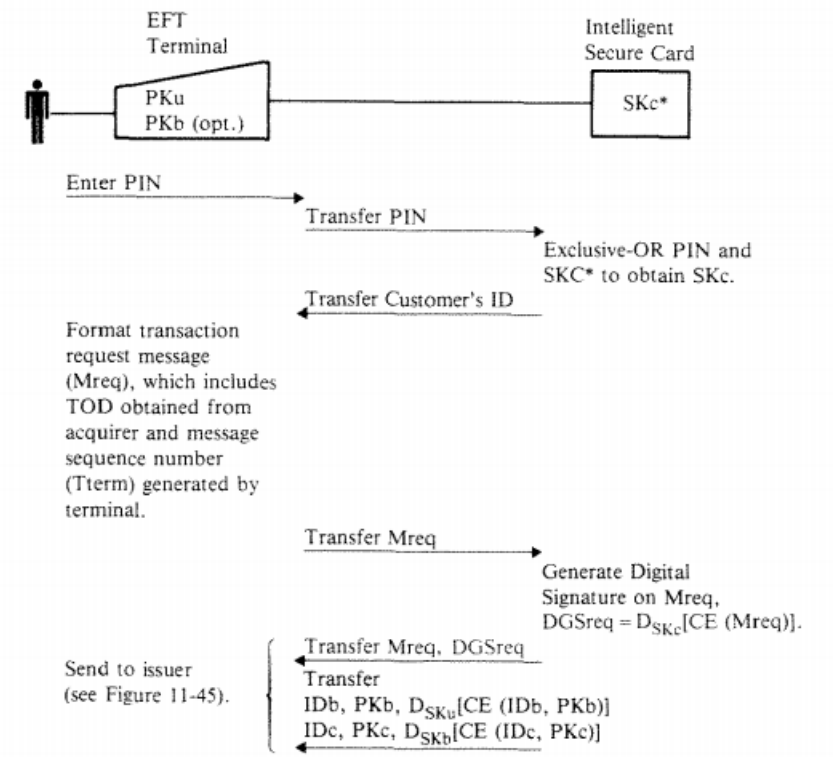


Figure 11-44. On-Line Use—EFT Terminal

Figure 11-44 depicts the receipt by an Intelligent Secure Card of a transaction request message (Mreq), which includes transaction information, after which the Intelligent Secure Card generates digital signature DGS using the user's private key SKc. Ex. 1022, 597.

2. Analysis of Asserted Ground of Anticipation by Meyer

Petitioner contends Meyer discloses each limitation of the four challenged claims. Pet. 35–50. Petitioner cites multiple distinct embodiments disclosed in the

Meyer textbook in support of its anticipation challenge. *E.g.*, Pet. 35–38, 42–45. Specifically, Petitioner cites (i) a non-cryptographic grocery transaction, (ii) the use of a cryptographic message authentication code ("MAC"), and (iii) the use of digital signatures based on public key algorithms, for different limitations of independent claim 51 (Pet. 19–22, 35–38, 42–45), and in some instances, for the same limitations of claim 51, e.g., a non-secret credential being previously issued by a trusted party to at least one of the parties, and reciting receiving funds transfer information (Pet. 37–41). Patent Owner argues that, "Petitioner mixes unlinked embodiments within Meyer that do not relate to one another, to stitch together what it believes will work as an anticipation contention. In fact, the distinct embodiments are incommensurable." Prelim. Resp. 52.

We agree with Patent Owner. "For anticipation, it is not enough that the prior art reference discloses multiple, distinct teachings that the ordinary artisan might somehow combine to achieve the claimed invention." *In re Arkley*, 455 F.2d 586, 587–88 (CCPA 1972); *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). Petitioner cites to multiple and distinct portions of the Meyer textbook to disclose individual limitations of independent claim 51. None of the cited distinct embodiments — the non-cryptographic grocery transaction, or the cryptographic message authentication code ("MAC"), or the digital signature — is cited for each limitation of claim 51. For example, the non-cryptographic grocery transaction is not cited as disclosing the step of generating a VAN, the MAC generation is not cited as disclosing the step of transfer of funds, and the digital signature is not cited as disclosing the authentication of funds from an account associated with a first party to an account associated with a second party. Pet. 35–37, 41–44. Thus, we are not persuaded that Petitioner has demonstrated that it is more likely than not that it would prevail in establishing the

unpatentability of claims 51, 53, 55, and 56 as anticipated by Meyer.

E. Proposed Obviousness Over Davies and Meyer

Petitioner provides explanations of how Davies and Meyer teach or suggest the limitations of the four challenged claims. Pet. 50–66. For claims 51 and 53, Petitioner cites to Davies as in its arguments for proposed anticipation by Davies, and adds citations to Meyer for the generating step of the recited method, along with the sequence of the method whereby at least a portion of the receiving step occurs before the generating step. Pet. 50–63.

For dependent claim 55, Petitioner makes the same assertions for obviousness as in its argument for proposed anticipation by Davies, namely, that Davies teaches or suggests that the VAN is generated by an error detection code ("Davies describes that the signature ("VAN") on a message M is generated by signing H(M) using the sender's secret key, where H(M) is obtained by applying a one-way function H to the message"). Pet. 63–64; *see also* Pet. 69 ("Davies . . . suggest[s] that the signature, i.e., VAN, is based on a one-way function"). Although as stated above, this argument is insufficient to demonstrate that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as anticipated by Davies, we are persuaded that the combination of Davies and Meyer teach or suggest claim 55's limitations and that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as obvious over Davies and Meyer.

For dependent claim 56's limitations, Petitioner cites to Meyer's disclosure of a second VAN and of sending a "negative response" to the terminal if the requested transaction cannot be honored. Pet. 64–66; Ex. 1022, 597.

Patent Owner argues that because neither Davies nor Meyer anticipates the claims, "their combination cannot render the claims obvious." Prelim. Resp 56.

As described above, however, we are persuaded that Petitioner has demonstrated that it is more likely than not that it would prevail in establishing the anticipation of claims 51 and 53 by Davies. We further are persuaded that Davies and Meyer teach or suggest the limitations of claims 55 and 56. Patent Owner also argues Petitioner has not provided sufficient analysis of a reason to combine Davies with Meyer. Prelim. Resp. 57–58. Petitioner, however, provides articulated reasoning with rational underpinning for the reason to combine, stating that:

> [C]ombining Davies with Meyer demonstrates that all the elements at issue were known in the prior art, and their combination yielded nothing but predictable results. Both references address methods for facilitating financial transactions and for providing data security for electronic funds transfer. Davies' method uses "a digital signature facility with a key registry to authenticate public keys," and to approve transactions. Davies at 328-331. Meyer similarly discloses using a message authentication code, or equivalently a digital signature in the context of public-key algorithms, to approve or disapprove transaction requests. Meyer at 457-58, 469 and 590. Applying the Meyer process of having an originator generate MACs after receiving transaction information to Davies would have yielded predicable results: using the Davies token to first receive the funds transfer information to then generate the VAN. *See KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 416 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). Thus, these references in their similar purpose of dealing with financial transactions and services, and overlapping teachings, confirm a motivation to combine Davies and Meyer.

Pet. 22–23 (citing to Ex. 1020 ¶¶ 112–18); Pet. 51. We have reviewed Petitioner's analysis and supporting evidence regarding this proposed ground of obviousness and, based on the record before us at this stage, we are satisfied that Petitioner's articulated reasoning is supported by sufficient rational underpinnings. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (an apparent reason to combine known elements in the fashion claimed by the patent at issue should be made

explicit). On the record before us, we are persuaded that Petitioner has demonstrated that it is more likely than not that it would prevail in establishing the unpatentability of claims 51, 53, 55, and 56 as obvious over Davies and Meyer.

F. Claim 55: Proposed Obviousness Over Davies and Nechvatal

1. Overview of Nechvatal

Nechvatal is titled "Public-key Cryptography," and describes, among other things, the use of digital signatures and hash functions in public key cryptography. Ex. 1006, §§ 1–3. According to Nechvatal, usually it is not desirable to apply a signature directly to a long message. *Id.* § 3.2. Accordingly, Nechvatal discloses the use of hash function, *H*, to accept a variable size message, *M*, as input, to produce a fixed-size representation, *H(M)*, as output. *Id*. Nechvatal discloses that, in general, *H(M)* will be much smaller than *M*, and, thus, a digital signature can be applied to *H(M)* in a relatively quick fashion. *Id*. Nechvatal further discloses that the "hash function can also serve to detect modification of a message, independent of any connection with signatures," and, thereby, the hash function "can serve as a cryptographic checksum." *Id*.

2. Analysis of Proposed Ground of Obviousness Over Davies and Nechvatal

Petitioner argues that claim 55 would have been obvious over Davies and Nechvatal. Pet. 66–69. Specifically, Petitioner argues that Davies's signatures may be generated by computing hash values on the transaction information as an intermediate step. *Id.* at 66. Furthermore, Petitioner relies upon Nechvatal for its disclosures regarding the use of hash functions to mitigate the effects of data expansion and lower bandwidth transmission that result from generating digital signatures. *Id*. Additionally, Petitioner proposes that Davies be combined with Nechvatal to allow the signing entity in Davies to condense the information *M*

included in a certificate into a fixed size representation *H(M)* that is of smaller size than *M*, and sign *H(M)* in a relatively quick fashion, which would improve signing efficiency, as taught by Nechvatal. *Id*. at 66–67. Finally, Petitioner states that while Davies "suggests that the signature, i.e., VAN, is based on a one-way function, Nechvatal explicitly mentions that the one-way function is an error detection code . . . Nechvatal discloses that a signature ('VAN') is generated using a hash function, which is an error detection code." *Id.* at 69.

Patent Owner argues "the Petition does not assert a proper 'reason to combine,'" but concedes Davies and Nechvatal "might overlap in certain teachings." Prelim. Resp. 60. Petitioner, however, explains that Nechvatal's hash functions improve signing efficiency and that it would be obvious for a person of ordinary skill in the art to combine the teachings of Davies "with Nechvatal to implement an electronic funds transfer system in which the transactions are authenticated by digital signatures, as taught by Davies." Pet. 67.

We have reviewed Petitioner's analysis and supporting evidence regarding this proposed ground of obviousness. On the record before us, we are persuaded that Petitioner has demonstrated that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 55 as obvious over Davies and Nechvatal.

G. Claim 56: Proposed Obviousness Over Davies, Fischer, and Piosenka

1. Overview of Fischer

Fischer is titled "Public Key/Signature Cryptosystem with Enhanced Digital Signature Certification," and discloses a public key cryptographic system with a hierarchy of nested certifications and signatures. Ex. 1007, Abstract.

Figure 3 of Fischer is reproduced below.

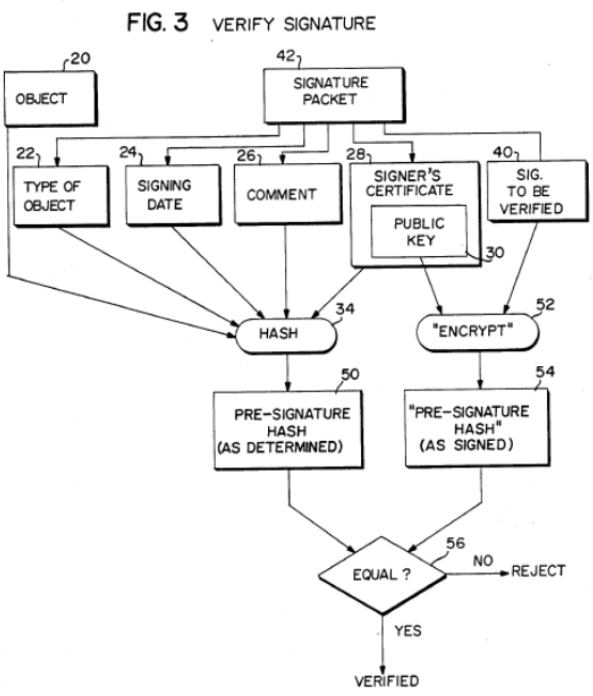


Figure 3 of Fischer above illustrates how a recipient of a transmitted message, including signature packet 42, verifies the signature. *Id.* at 11:45–48. Fischer discloses that the recipient applies hashtag algorithm 34 to the signature packet and associated fields 22, 24, 26, and 28 to result in presignature hash 50. *Id.* at 11:48–53. Fischer discloses that the recipient then utilizes the public encrypting key transmitted with the signer's certificate, which certificate was transmitted with the signature packet, and performs encrypt (verification) operation 52 on the signature to be verified 40 to generate presignature hash 54. *Id.* at 11:54–58. The recipient then compares this value with the encryption (verification) of the signer's signature. *Id.* at 11:59–61.

Fischer discloses that, in accordance with the procedure detailed in Figure 3, the recipient ensures that each signature includes a corresponding validated certificate. *Id.* at 17:33–38. Furthermore, if the certificate requires joint

signatures, then the recipient ensures that the necessary signatures are present. *Id.* at 17:40–41.

2. Overview of Piosenka

Piosenka is titled "Unforgeable Personal Identification System," and discloses a system for identifying users at remote access sites. Ex. 1008, Abstract. Piosenka discloses that a user's credentials can be stored on a portable memory device from which the encrypted identification credentials can be read. *Id.* Piosenka discloses that, in its validation procedure, the memory medium is read, and the information is decrypted using the public decryption key. *Id.* at 11:14–17. Furthermore, Piosenka discloses a comparison of whether the calculated cryptographic signature matches the cryptographic signature recorded on the memory medium, and, if they do not match, the "request is denied and the process ended." *Id.* at 11:17–23.

3. Analysis of Proposed Obviousness Over Davies, Fischer, and Piosenka

Petitioner argues that claim 56 would have been obvious over Davies, Fischer, and Piosenka. Pet. 69–76. Claim 56 is dependent from claim 51 and includes the requirement that "the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1." Petitioner cites to Fischer's disclosure regarding a signature verification procedure that includes a hierarchy of certificates as teaching the claimed "second variable authentication number (VAN1)." Pet. 70 (citing Ex. 1006, 17:34–47). Furthermore, Petitioner

cites to Piosenka's disclosure of denying a user's request for access if the signature on the user's credential cannot be validated as teaching the claimed "funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1." Pet. 71, 75–76 (citing Ex. 1008, 6:41–42, 11:15–23).

Patent Owner argues "the asserted 'reason to combine'" is insufficient. Prelim. Resp. 62. Petitioner, however, explains that:

> A person of ordinary skill in the art would be motivated, at the time of the effective filing date of the '302 Patent, to combine the teachings of Davies with the teachings of Fischer for securing messages, end-to-end. . . . It would also be obvious for a person of ordinary skill in the art to augment the authenticated electronic funds transfer mechanisms using digital signatures, which is taught by Davies, with the counter signature of Fischer, as this would allow for the electronic funds transfer transaction using a chain of authority, where each higher level approves any commitment/signature made at a lower level. . . . A person of ordinary skill in the art would be motivated, at the time of filing the application to which the '302 Patent claims priority, to augment the verification of message signatures and public keys, as taught by the combination of Davies and Fischer, with the denial of request upon failure to verify the user's credential, as taught by Piosenka.

Pet. 69–71 (citing Ex. 1020 ¶¶ 158–60, 174). We have reviewed Petitioner's analysis and supporting evidence regarding this proposed ground of obviousness and, based on the record now before us, we are satisfied that Petitioner's articulated reasoning is supported by sufficient rational underpinnings. *See KSR*, 550 U.S. at 418 (an apparent reason to combine known elements in the fashion claimed by the patent at issue should be made explicit). On the record before us, we are persuaded that Petitioner has demonstrated that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claim 56 as obvious over Davies, Fischer, and Piosenka.

III. CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition establishes that it is more likely than not that Petitioner would prevail in establishing the unpatentability of claims 51, 53, 55, and 56 of the '302 patent.

The Board has not made a final determination on the patentability of the challenged claims.

IV. ORDER

For the reasons given, it is

ORDERED that a covered business method patent review is instituted on the following grounds:

1. Claims 51 and 53 under 35 U.S.C. § 102 as anticipated by Davies;

2. Claims 51, 53, 55, and 56 under 35 U.S.C. § 103(a) as obvious over Davies and Meyer;

3. Claim 55 under 35 U.S.C. § 103(a) as obvious over Davies and Nechvatal;

4. Claim 56 under 35 U.S.C. § 103(a) as obvious over Davies, Fischer, and Piosenka;

FURTHER ORDERED that pursuant to 35 U.S.C. § 324(d) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial commencing on the entry date of this Order.

PETITIONER:

Robert C. Scheinfeld
robert.scheinfeld@bakerbotts.com

Eliot D. Williams
eliot.williams@bakerbotts.com

PATENT OWNER:

Robert Greenspoon
rpg@fg-law.com

John Fitzgerald
patents@rutan.com