IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
CASE NO.: 14-60830-CIV-MOORE

LEON STAMBLER,

Plaintiff,

v.

MASTERCARD INCORPORATED (d/b/a MASTERCARD WORLDWIDE) and MASTERCARD INTERNATIONAL INCORPORATED,

Defendants.
_____/

DEFENDANTS MASTERCARD INCORPORATED AND MASTERCARD INTERNATIONAL INCORPORATED'S INVALIDITY CONTENTIONS

I. INTRODUCTION

Pursuant to the Court's Patent Pretrial Order (Dkt. 23), dated May 15, 2014, Defendants Mastercard Incorporated and Mastercard International Incorporated (collectively, "MasterCard") hereby submit the following Invalidity Contentions with respect to the claims specifically identified by plaintiff Leon Stambler ("Stambler") in his Disclosure of Asserted Claims and Infringement Contentions, dated May 29, 2014. Stambler has charted claims 51, 53, 55, and 56 of U.S. Patent No. 5,793,302 ("the '302 patent") (collectively referred to as the "Asserted Claims").

With respect to each Asserted Claim and based on its investigation to date, MasterCard hereby: (a) identifies each currently known item of prior art that either anticipates or renders obvious each Asserted Claim; (b) specifies whether each such item of prior art (or a combination

of several of the same) anticipates each Asserted Claim or renders it obvious; (c) submits a chart identifying where each element in each Asserted Claim is disclosed, described, or taught in the prior art, including for each element that is governed by 35 U.S.C. § 112 ¶ 6, the identity of the structure(s), act(s), or material(s) in each item of prior art that performs the claimed function; (d) specifies how each of the Asserted Claims is invalid for failing to claim patentable subject matter under 35 U.S.C. § 101; and (e) identifies the grounds for invalidating Asserted Claims based on indefiniteness under 35 U.S.C. § 112 ¶ 2 or lack of enablement or lack of written description under 35 U.S.C. § 112 ¶ 1.

II. RESERVATIONS

Consistent with the Patent Pretrial Order in this case, MasterCard reserves the right, upon leave of the Court, to amend these Invalidity Contentions.

MasterCard expressly reserves the right to amend these disclosures should plaintiff be allowed to assert additional claims, should plaintiff provide any information that it failed to provide in its Disclosure of Asserted Claims and Infringement Contentions[1] or should plaintiff further amend its Disclosure of Asserted Claims and Infringement Contentions in any way. Further, because the case has just begun and because MasterCard has not yet completed its search for and analysis of relevant prior art, MasterCard reserves the right to revise, amend, and/or supplement the information provided herein, including identifying, charting, and relying on additional references, should MasterCard's further search and analysis yield additional information or references, consistent with the Patent Pretrial Order and the Federal Rules of Civil Procedure. Moreover, MasterCard reserves the right to revise its ultimate contentions

[1] For example, plaintiff's Disclosure of Asserted Claims and Infringement Contentions to MasterCard alleged the Asserted Claims are "entitled to a priority date at least as early as November 17, 1992." The Patent Pretrial Order, ¶ I(1)(f), requires plaintiff to provide the priority date for each asserted claim, not a reservation of rights for plaintiff to later claim an earlier date. MasterCard has relied on plaintiff's alleged November 17, 1992 priority date to form these Invalidity Contentions. Should Plaintiff later seek to rely on an earlier priority date, MasterCard reserves the right to amend these Invalidity Contentions.

concerning the invalidity of the Asserted Claims, which may change depending upon the Court's construction of the Asserted Claims, any findings as to the priority date of the Asserted Claims, and/or positions that plaintiff or expert witness(es) may take concerning claim construction, infringement, and/or invalidity issues.

Prior art not included in this disclosure, whether known or not known to MasterCard, may become relevant. In particular, MasterCard is currently unaware of the extent, if any, to which Stambler will contend that limitations of the Asserted Claims are not disclosed in the prior art identified by MasterCard. To the extent that such an issue arises, MasterCard reserves the right to identify other references that would render obvious the allegedly missing limitation(s) of the disclosed method.

MasterCard further intends to rely on inventor admissions concerning the scope of the prior art relevant to the asserted claims found in, *inter alia*: the patent prosecution history for the asserted patent and related patents and/or patent applications; any deposition testimony or declarations of the named inventor on the asserted or related patents; and the papers filed and any evidence submitted by Stambler in connection with this litigation or in any other past, pending, or future litigations brought by Stambler involving the '302 patent.

MasterCard's claim charts cite particular teachings and disclosures of the prior art as applied to features of the Asserted Claims. However, persons having ordinary skill in the art generally may view an item of prior art in the context of other publications, literature, products, and understanding. As such, the cited portions are only representative examples, and MasterCard reserves the right to rely on other, uncited portions of the prior art references and on other publications and expert testimony as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that the prior art discloses a

claim limitation or the invention as a whole. MasterCard further reserves the right to rely on uncited portions of the prior art references, other publications, and testimony, including expert testimony, to establish bases for combinations of certain cited references that render the Asserted Claims obvious.

The references discussed in the claim charts may disclose the elements of the Asserted Claims explicitly and/or inherently, and/or they may be relied upon to show the state of the art in the relevant time frame. The suggested obviousness combinations are provided in the alternative to MasterCard's anticipation contentions and are not to be construed as suggesting that any reference included in any of the combinations is not by itself anticipatory.

MasterCard reserves the right to assert that the Asserted Claims are invalid under 35 U.S.C. § 102(f) in the event MasterCard obtains evidence that Leon Stambler, the inventor named in the asserted patents, did not invent (either alone or in conjunction with others) the alleged subject matter claimed in the Asserted Claims. Should MasterCard obtain such evidence, it will provide the name(s) of the person(s) from whom and the circumstances under which the invention or any part of it was derived.

MasterCard also reserves all of its rights to challenge any of the claim terms herein under 35 U.S.C. § 112, including by arguing that they are indefinite, not supported by the written description and/or not enabled. Accordingly, nothing stated herein shall be construed as a waiver of any argument available under 35 U.S.C. §§ 101 and 112.

III. INVALIDITY CONTENTIONS

A. Identification Of Prior Art (Tables 1 and 2)

Pursuant to the Patent Pretrial Order, ¶ I(2)(a), and subject to MasterCard's reservation of rights, MasterCard identifies each item of prior art that anticipates or renders obvious one or more of the Asserted Claims in Tables 1 and 2 below. Table 1 provides the full identity of each

listed prior art patent by patent number, country of origin, and date of issue. Table 2 provides the full identity of each listed non-patent prior art system or reference by title, date of publication, and, where feasible, author and publisher.

As this case has just begun, MasterCard's prior art investigation and third-party discovery is therefore not yet complete. MasterCard reserves the right to present additional items of prior art under 35 U.S.C. § 102(a), (b), (e), and/or (g), and/or § 103 located during the course of discovery or further investigation. For example, MasterCard expects to issue subpoenas to third parties believed to have knowledge, documentation and/or corroborating evidence concerning at least some of the prior art listed in Tables 1 and 2 and/or additional prior art. These third parties include without limitation the authors, inventors, or assignees of the references listed in these disclosures. In addition, MasterCard reserves the right to assert invalidity under 35 U.S.C. § 102(c), (d), or (f) to the extent that discovery or further investigation yields information forming the basis for such invalidity.

Table 1: Prior Art Patents

Patent (Primary Inventor)	Filing Date; Date of Issue/ Publication	Short Name
CA 2175716 (Weiss et al.)	Nov. 8, 1990; May 9, 1992	CA Weiss
EP 0119707A1 (Serpell)	Feb. 6, 1984	EP Serpell 707
EP 0500245A2 (Lijima)	Feb. 7, 1992	EP Lijima
EP 140388A2 (Atalla)	Oct. 31, 1984; May 8, 1985	EP Atalla
EP 174016A2 (Kawana)	Sep. 4, 1985; Mar. 12, 1986	EP Kawana
EP 186981B1 (Smith)	Dec. 4, 1985; July 9, 1986	EP Smith
EP 0225010 (Serpell)	Sep. 26, 1986	EP Serpell

Patent (Primary Inventor)	Filing Date; Date of Issue/ Publication	Short Name
EP 0246823 (Beker)	May 18, 1987; Nov. 25, 1987	EP Beker
EP 254595A2 (Mcquire)	July 24, 1987; Jan. 27, 1988	EP Mcquire
EP 292247A2 (McDonald)	May 18, 1988; Nov. 23, 1988	EP McDonald
EP 0386897 (Harada)	Feb. 15, 1990	EP Harada
EP 426507A2 (Benton)	Sep. 14, 1990; May 8, 1991	EP Benton
EP 481135A1 (Josephson)	Oct. 17, 1990; Apr. 22, 1992	EP Josephson
EP 504287A1 (Lawlor)	Dec. 10, 1990; Sep. 23, 1992	EP Lawlor
EP 98593A2 (Nagata)	July 5, 1983; Jan. 18, 1984	EP Nagata
GB 2011671A (Stuckert)	Nov. 23, 1978; Jul. 11, 1979	GB Stuckert
GB 2079504A (Campbell)	Jul. 1, 1980; Jan. 29, 1982	GB Campbell
GB 2100190A (Scheffel)	Jun. 3, 1982; Dec. 22, 1982	GB Scheffel
GB 2102606A (Bell)	Jun. 17, 1982; Feb. 2, 1983	GB Bell
GB 2155675A (Croft)	Feb. 19, 1985; Sep. 25, 1985	GB Croft
GB 2188180A (Victor)	Mar. 23, 1987; Sep. 23, 1987	GB Victor
GB 2212641A (Johnson)	July 12, 1988; July 26, 1989	GB Johnson
GB 2251098A (McHugh)	Dec. 17, 1990; June 24, 1992	GB McHugh
IE 49937B1 (Interbank Card Association)	July 3, 1980; Jan. 8, 1986	IE ICA
U.S. Patent No. 3,956,615 (Anderson et al.)	June 25, 1974; May 11, 1976	Anderson
U.S. Patent No. 3,990,558 (Ehrat)	Oct. 7, 1974; Nov. 9, 1976	Ehrat
U.S. Patent No. 4,200,770 (Hellman et al.)	Sept. 6, 1977; Apr. 29, 1980	Hellman ’770
U.S. Patent No. 4,218,582 (Hellman et al.))	Oct. 6, 1977; Aug. 19, 1980	Hellman ’582

Patent (Primary Inventor)	Filing Date; Date of Issue/ Publication	Short Name
U.S. Patent No. 4,253,158 (McFiggans)	Mar. 28, 1979; Feb. 24, 1981	McFiggans
U.S. Patent No. 4,259,720 (Campbell)	Jan. 9, 1978; Mar. 31, 1981	Campbell
U.S. Patent No. 4,264,782 (Konheim)	Jun. 29, 1979; Apr. 28, 1981	Konheim
U.S. Patent No. 4,302,810 (Bouricius et al.)	Dec. 28, 1979; Nov. 24, 1981	Bouricius
U.S. Patent No. 4,305,059 (Benton)	Jan. 3, 1980; Dec. 8, 1981	Benton
U.S. Patent No. 4,315,101 (Atalla)	Oct. 9, 1979; Feb. 9, 1982	Atalla ’101
U.S. Patent No. 4,357,529 (Atalla)	Nov. 17, 1980; Nov. 2, 1982	US Atalla or Atalla ’529
U.S. Patent No. 4,376,299 (Rivest)	Jul. 14, 1980; Mar. 8, 1983	Rivest ’299
U.S. Patent No. 4,390,968 (Henessey et al.)	Dec. 30, 1980; June 28, 1983	Henessey
U.S. Patent No. 4,405,829 (Rivest et al.)	Dec. 14, 1977; Sept. 20, 1983	Rivest ’829
U.S. Patent No. 4,424,414 (Hellman et al.)	May 1, 1978; Jan. 3, 1984	Hellman ’414
U.S. Patent No. 4,500,750 (Elander et al.)	Dec. 30, 1981 Feb. 19, 1985	Elander
U.S. Patent No. 4,630,201 (White)	Feb. 14, 1984; Dec. 16, 1986	White
U.S. Patent No. 4,633,037 (Serpell)	Feb. 21, 1984; Dec. 30, 1986	Serpell
U.S. Patent No. 4,652,698 (Hale et al.)	Aug. 13, 1984 Mar. 24, 1987	Hale
U.S. Patent No. 4,720,860 Weiss	Nov. 30, 1984 Jan. 19, 1988	Weiss
U.S. Patent No. 4,747,050 (Brachtl et al.)	Aug. 28, 1987; May 24, 1988	Brachtl ’050
U.S. Patent No. 4,755,940 (Brachtl et al.)	Jan. 6, 1987; Jul. 5, 1988	Brachtl ’940
U.S. Patent No. 4,771,461 (Matyas)	Jun. 27, 1986; Sept. 13, 1988	Matyas ’461
U.S. Patent No. 4,775,246 (Edelmann et al.)	Feb. 25, 1986; Oct. 4, 1988	Edelmann
U.S. Patent No. 4,796,193 (Pitchenik)	Jul. 7, 1986; Jan. 3, 1989	Pitchenik

Patent (Primary Inventor)	Filing Date; Date of Issue/ Publication	Short Name
U.S. Patent No. 4,825,050 (Griffith et al.)	Sep. 13, 1983; Apr. 25, 1989	Griffith
U.S. Patent No. 4,849,613 (Eisele)	May 13, 1985; Jul. 18, 1989	Eisele
U.S. Patent No. 4,868,877 (Fischer)	Feb. 12, 1988; Sep. 19, 1989	Fischer ’877
U.S. Patent No. 4,885,777 (Takaragi et al.)	Apr. 11, 1988; Dec. 5, 1989	Takaragi ’777
U.S. Patent No. 4,890,323 (Beker et al.)	May 20, 1987; Dec. 26, 1989	Beker
U.S. Patent No. 4,910,676 (Alldredge)	Mar. 30, 1987; Mar. 20, 1990	Alldredge
U.S. Patent No. 4,912,762 (Lee et al.)	Apr. 18, 1988; Mar. 27, 1990	Lee
U.S. Patent No. 4,914,698 (Chaum)	Jul. 24, 1989; Apr. 3, 1990	Chaum ’698
U.S. Patent No. 4,926,480 (Chaum)	May 24, 1988; May 15, 1990	Chaum ’480
U.S. Patent No. 4,949,380 (Chaum)	Oct. 20, 1988; Aug. 14, 1990	Chaum ’380
U.S. Patent No. 4,962,531 (Sipman et al.)	Aug. 26, 1988; Oct. 9, 1990	Sipman
U.S. Patent No. 4,984,270 (LaBounty)	Jun. 19, 1987; Jan. 8, 1991	LaBounty
U.S. Patent No. 4,993,068 (Piosenka et al.)	Nov. 27, 1989 Feb. 12, 1991	Piosenka
U.S. Patent No. 5,005,200 (Fischer)	Mar. 7, 1989; Apr. 2, 1991	Fischer ’200
U.S. Patent No. 5,012,076 (Yoshida)	Mar. 1, 1989; Apr. 30, 1991	Yoshida
U.S. Patent No. 5,018,196 (Takaragi et al.)	Jul. 5, 1989; May 21, 1991	Takaragi ’196
U.S. Patent No. 5,020,105 (Rosen et al.)	Aug. 17, 1989 May 28, 1991	Rosen ‘105
U.S. Patent No. 5,068,894 (Hoppe)	Aug. 22, 1990 Nov. 26, 1991	Hoppe
U.S. Patent No. 5,081,676 (Chou et al.)	Oct. 4, 1990 Jan. 14, 1992	Chou
U.S. Patent No. 5,175,416 (Mansvelt et al.)	May 17, 1991; Dec. 29, 1992	Mansvelt
U.S. Patent No. 5,336,870 (Hughes et al.)	May 26, 1992; Aug. 9, 1994	Hughes

Patent (Primary Inventor)	Filing Date; Date of Issue/ Publication	Short Name
U.S. Patent No. 5,432,506 (Chapman)	Feb. 25, 1992; Jul. 11, 1995	Chapman
U.S. Patent No. 5,453,601 (Rosen)	Nov. 15, 1991; Sept. 26, 1995	Rosen
U.S. Patent No. 5,534,855 (Shockley, et al.)	Dec. 15, 1994; Jul. 9, 1996	Shockley
WO 198503787 (White)	Feb. 5, 1985; Aug. 29, 1985	WO White
WO 1986000441A1 (Scheurer)	June 25, 1985; Jan. 16, 1986	WO Scheurer
WO 1990000281A1 (Keyser et al.)	June 30, 1989; Jan. 11, 1990	WO Keyser
WO 1991007725A2 (Small et al.)	Nov. 20, 1990; May 30, 1991	WO Small
U.S. Patent No. 5,369,705 (Bird, et al.)	June 3, 1992; Nov. 29, 1994	Bird
U.S. Patent No. 4,734,858 (Schlafly)	Nov. 26, 1984; Mar. 29, 1988	Schlafly
WO 84/04639 (Edstrom)	May 6, 1983 Nov. 22, 1984	Edstrom
WO 91/14980 (Glaschick)	Mar. 20, 1990 Oct. 3, 1991	Glaschick
WO 91/16691 (Jones, et al.)	April 10, 1991; Oct. 31, 1991	Jones

Table 2: Non-Patent Prior Art

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Accredited Standards Committee X9—Financial Services	American National Standard (ANSI), Financial Institution Key Management (Wholesale) X9.17 (April 4, 1985).	1985	ANSI X9.17
Accredited Standards Committee X9—Financial Services	American National Standard (ANSI), Financial Institution Message Authentication (Retail) X9.19 (August 13, 1986).	1986	ANSI X9.19

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Accredited Standards Committee X9—Financial Services	American National Standard (ANSI), Financial Institution Message Authentication (Wholesale) X9.9 (August 15, 1986).	1986	X9.9-1986
Accredited Standards Committee X9—Financial Services	American National Standard (ANSI), Financial Institution Message Authentication X9.9 (April 13, 1982).	1982	ANSI X9.9 1982
Selim G. Akl	S. G. Akl, Digital Signatures: A Tutorial Survey, in Computer, 15 (Feb. 1983)	1983	Akl
ABA Banking Journal	Beware! Fax attacks!, American Bar Association (ABA) Banking Journal, June 1990, p. 52-60	1990	ABA
Michael S. Baum and Henry H. Perritt	Electronic Contracting, Publishing and EDI Law	1991	Baum-1991
Henry Beker	H. Beker, The User of Automated Cryptographic Check-Sums, IFIP Computer Security in the Age of Information 75 (1989).	1989	Beker Paper
Henry Beker & Michael Walker	Henry Beker & Michael Walker, Key Management for Secure Electronic Funds Transfer in a Retail Environment, Advances in Cryptology: Proceedings of CRYPTO 84 (1985).	1985	Beker & Walker
Luigia Berardi	L. Berardi, Some Remarks about an Electronic Signature Derived from a Generalized RSA-Code, 11 J. Inf. Optimization Sci. 189 (1990).	1990	Berardi
Albrecht Beutelspacher & Thomas Hueske Payment	Payment Applications with Multifunctional Smart Cards," Proceedings of the IFIP WG 11.6 International Conference on SMART CARD 2000: The Future of IC Cards, Laxenaburg, Austria, October 19-20, 1987	1989	Beutelspacher Article
Robert C. Blattberg	R. Blattberg, Interactive Marketing: Exploiting the Age of Addressability, 33 Sloan Management Review 5 (1991)	1991	Blattberg

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Burk et al.	Burk et al., Value Exchange Systems Enabling Security and Unobservability, 9 Computers & Security 715 (1990)	1990	Burk
Holger Burk & Andreas Pfitzmann	Burk & Pfitzmann, "Digital Payment Systems Enabling Security and Unobservability," 8 Computers & Security 399 (1989)	1989	Burk II
Torrey Byles	T. Byles, More Companies Are Paying Bills Electronically, The Journal of Commerce (May 5, 1988)	1988	Byles
Carl Campbell	C. Campbell, Design and Specification of Cryptographic Capabilities, 16 Comm. Mag. 15 (Nov. 1978).	1978	Campbell Paper
Carl Campbell	C. Campbell, A Microprocessor-Based Module to Provide Security in Electronic Funds Transfer Systems, IEEE (1979)	1979	Campbell II
J.D. Carreker	J.D. Carreker, Strides in Electronic Checking Transforming Payment System, Bank Management 18 (March 1992)	1992	Carreker
David Chaum	D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete, 28 Communications of the ACM 1030 (Oct. 1985)	1985	Chaum I
David Chaum	D. Chaum, A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations, Advances in Cryptology –CRYPTO '86, 118-167 (1987)	1987	Chaum II
Checkfree	Checkfree: The Nation's Electronic Bill Payment System User Manual 3.0 Version	1991	CheckFree User Manual
David Churbuck	D. Churbuck, Let Your Fingers Do the Banking, (Use of Computers for Electronic Banking from Home), 122 Forbes (1991)	1991	Churbuck
J. Cobb	J. Cobb, Security Implications for EDI, IEEE Colloquium on Standards and Practices in Electronic Data Interchange (May 1991)	1991	Cobb

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
John C. Comfort & Pamela K. Coats	J. Comfort & P. Coats, Electronic Funds Transfer Networks: The Impact of Performance and Security Considerations, Annual Simulation Symposium, 1980	1980	Comfort
Committee IS/5, Electronic Funds Transfer	Electronic Funds Transfer—Requirements for Interfaces: Part 4—Message Authentication (May 1985)	1985	IS/5
Whitfield Diffie and Martin E. Hellman	W. Diffie & M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976	1976	Diffie II
Craig Crossman	C. Crossman, Paying Bills Can Be an Electronic Task, Miami Herald, Mar. 12 1990	1990	Crossman
Whitfield Diffie	W. Diffie, The First Ten Years of Public-Key Cryptography, 76 Proceedings of the IEEE 560, (May 1988)	1988	Diffie Paper
D. W. Davies & W. J. Price	D. W. Davies & W. J. Price, Security for Computer Networks (John Wiley & Sons) (2d ed. 1989)	1989	Davies I
Donald Watts Davies	D. W. Davies, The Use of Digital Signatures in Banking, Proceedings of the 2nd IFIP International Conference on Computer Security: A Global Challenge 13 (1984).	1984	Davies II
Donald Watts Davies	D. W. Davies, Applying the RSA Digital Signature to Electronic Mail, 16 Computer 55 (Feb. 1983)	1983	Davies III
Donald Watts Davies	D. W. Davies, A Message Authenticator Algorithm Suitable for a Mainframe Computer, Proceedings of CRYPTO 84 on Advances in Cryptology, 393 (1985).	1985	Davies IV
D. W. Davies & W. L. Price	D.W. Davies & W.L. Price, The Application of Digital Signatures Based on Public Key Cryptosystems, NPL Report (1980)	1980	Davies V
Daniel P. Dern	Daniel P. Dern, Guarding Company Network Transmissions and Storage, InfoWorld, p. S6 (1989).	1989	InfoWorld

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Sam Diamond	S. Diamond, Check Processing Takes a New Turn, Computers in Banking 50 (March 1988)	1988	Diamond
Semyon Dukach	S. Dukach, SNPP: A Simple Network Payment Protocol, Proceedings of the Eighth Annual Computer Security Applications Conference 173 (1992).	1992	Dukach
Online Resources	Online Resources & Communications Corporation	1993	Screenphone Offering
ASC X12 Standards Committee	Electronic Data Interchange X12 Standards, Draft Version 3, Release 2, Volumes I & II	1991	EDI
Ken J. Fifield	K. Fifield, Smartcards Outsmart Computer Crime, 8 Computers & Security 247 (1989)	1989	Fifield
Addison M. Fischer	A. Fischer, Electronic Document Authorization, Proc. IFIPWG 6.5, Int. Symposium, Zurich (1990).	1990	Fischer Paper
Jacqueline Floch	J. Floch, Privacy Protected Payments – An Implementation of a Transaction System, ELAB-RUNIT (Dec 1988)	1988	Floch
Jason Gait	J. Gait, Communications Security for Electronic Funds Transfer Systems, IEEE Journal on Selected Areas in Communications (Vol. Sac-2, No. 3) (May 1984)	1984	Gait
Morrie Gasser	The Digital Distributed System Security Architecture	1989	Gasser
Dahl Gerberick	Working Paper On Functional Specifications For An EDI Cryptoserver	1989	Gerberick
Fr. M. Blake Greenlee	Fr. M. Blake Greenlee, Requirements for Key Management Protocols in the Wholesale Financial Services Industry, 23 IEEE Comm. Mag. 22 (Sept. 1985)	1985	Greenlee
Ralph Gyoery & Jennifer Seberry	R. Gyoery & J. Seberry, Electronic Funds Transfer Point of Sale in Australia, CRYPTO 347 (1986).	1986	Gyoery
Harold J. Highland	Harold J. Highland, Encryption Packages Offer Business Users a Choice, Computerworld, p. S5 (1987)	1987	Computerworld

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
J. Linn	IAB Privacy Task Force, Network Working Group, Request for Comments: 1113, Privacy Enhancement for Internet Electronic Mail - Message Encipherment and Authentication Procedures (August 1989)	1989	RFC 1113 (Collectively, RFC 1113, 1114, and 1115 are referred to herein as "PEM-1989").
S. Kent J. Linn	IAB Privacy Task Force, Network Working Group, Request for Comments: 1114, Privacy Enhancement for Internet Electronic Mail: Certificate-Based Key Management (August 1989)	1989	RFC 1114 (Collectively, RFC 1113, 1114, and 1115 are referred to herein as "PEM-1989").
J. Linn	IAB Privacy Task Force, Network Working Group, Request for Comments: 1114, Privacy Enhancement for Internet Electronic Mail: Algorithms, Modes, and Identifiers (August 1989)	1989	RFC 1115 (Collectively, RFC 1113, 1114, and 1115 are referred to herein as "PEM-1989").
IBM Technical Disclosure Bulletin	27 Personal Authentication Code Generation 5576-5578 (Mar. 1985)	1985	IBM I
IBM Technical Disclosure Bulletin	28 Personal Key Implementation with Standardized Bank Cards 4375-4377 (Mar. 1986)	1986	IBM II
International Organization for Standardization	International Organization for Standardization (ISO), Banking – Requirements for Message Authentication (Wholesale) ISO 8730 (May 15, 1990)	1990	ISO 8730
International Organization for Standardization	International Organization for Standardization (ISO), Banking and Related Financial Services – Requirements for Message Authentication (Retail) ISO 9807 (Dec. 15, 1991)	1991	ISO 9807
International Telegraph and Telephone Consultative Committee (CCITT)	CCITT, Series X: Data Communication Networks: Directory, The Directory – Authentication Framework, X.509 (Nov. 1988)	1988	X.509

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Loren M Kohnfelder	L. Kohnfelder, Towards a Practical Public-Key Cryptosystem, Massachusetts Institute of Technology (1978).	1978	Kohnfelder Thesis
Alan G. Konheim	A. Konheim, A One-Way Sequence for Transaction Verification, IBM Thomas J. Watson Research Center (1981).	1981	Konheim Paper
Richard Lennon et al.	R. Lennon et al., Cryptographic Authentication of Time-Invariant Quantities, 29 IEEE Transaction on Communications 773 (1981)	1981	Lennon
Christor Linden & Hans Block	C. Linden & H. Block, Sealing Electronic Money in Sweden, 1 Computers & Security 226 (1982).	1982	Linden
Luc Longpré	L. Longpré, The Use of Public-Key Cryptography for Signing Checks, CRYPTO 187 (1982).	1982	Longpre
Lubold et al.	Lubold et al., Transaction Completion Code Based on Digital Signatures, 28 IBM Technical Disclosure Bulletin 1109 (Aug. 1985)	1985	Lubold
Stephen M. Matyas	S.M. Matyas, Public Key Registration, Lecture Notes in Computer Science, 1987, Vol. 263, Advances in Cryptology – CRYPTO 86, p. 451-458.	1986	Matyas Paper
C.H. Meyer & S.M. Matyas	C.H Meyer & S.M. Matyas, Some Cryptographic Principles of Authentication in Electronic Funds Transfer Systems, Proceedings of the Seventh Symposium on Data Communications (1981).	1981	Meyer I
C.H. Meyer & S.M. Matyas	C.H. Meyer & S.M Matyas, Cryptography: A New Dimension in Computer Data Security (1982)	1982	Meyer II or Matyas 1982
C.H. Meyer et al.	C.H. Meyer et al., Required Cryptographic Authentication Criteria for Electronic Funds Transfer Systems, IEEE (1981)	1981	Meyer III
Sead Muftic	S. Muftic, Security Mechanisms for Computer Networks, 15 Computer Networks 67 (1988).	1988	Muftic

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Internet Engineering Task Force	Kerberos Network Authentication Service as publicly known and used and described in at least (1) The Kerberos Network Authentication Service: Request for Comments: Draft 4, December 20, 1990; (2) Kerberos: An Authentication Service for Open Network Systems, Published March 30, 1988, (3) The Kerberos Network Authentication Service (V5), published September 1, 1992, (4) Kerberos: An Authentication Service for Open Network Systems, published February 9-12, 1988, and (5) The Three-Headed Dog, published May 31, 1990	1988	Kerberos
National Institute of Standards and Technology	N.I.S.T., A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), 56 Fed. Reg. 42980 (Aug. 30, 1991)	1991	DSS
James Nechvatal	J. Nechvatal, Public-key Cryptography, (NIST special publication, Apr. 1991)	1991	Nechvatal
B. Clifford Neuman	B.C. Neuman, Proxy-Based Authorization and Accounting for Distributed Systems, Technical Report 91-02-01 (Mar. 1991)	1991	Neuman
Omaha World Herald	Banks, Credit Unions Join in Utilities to Expand Bill Payment Plan, Omaha World – Herald, Aug. 30, 1989, at 19.	1989	Omaha
Birgit Pfitzmann	B. Pfitzmann, Fail-stop Signatures; Principles and Applications, Proc. Compsec ’91 125 (1991).	1991	Pfitzmann
Lawrence Reeves	L. Reeves, Protecting Electronic Funds Transfers with Secure Data Communications and Dynamic Signature Analysis, Queen’s University (Sep. 1990)	1990	Reeves
Karl Rihaczek	K. Rihaczek, Teletrust, 13 Computer Networks & ISDN Systems 235 (1987).	1987	Rihaczek
U. Rimensberger	U. Rimensberger, Encryption: Needs, Requirements and Solutions in Banking Networks, EUROCRYPT 1985 (1986).	1986	Rimensberger

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Bank Administration Institute	Network Security Techniques for Financial Institutions	1990	BAI
R. L. Rivest, et al.,	R. L. Rivest et al., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, 21 Communications of the ACM 120 (Feb. 1978)	1978	Rivest Paper or Rivest '78
R. Rivest	R. Rivest, The MD4 Message Digest Algorithm, Network Working Group Request for Comments: 1186 (Oct. 1990)	1990 Rivest	MD4
S.C. Serpell	S.C. Serpell, Electronic Funds Transfer Security: A Network-Optimised Approach, 20 Electronic Letters 836 (Sept. 1984)	1984	Serpell Paper
Michael Shain	M. Shain, Security in Electronic Funds Transfer, 8 Computers & Security 209 (1989)	1989	Shain
Chris Shipley	C. Shipley, I Threw Away My Checkbook, PC Computing (Nov. 1990)	1990	Shipley
Gustavus J. Simmons	G. Simmons, A System for Point-of-Sale or Access Under User Authentication and Identification, CRYPTO 1981, 31 (1982)	1982	Simmons I
Gustavus J. Simmons	G. Simmons, The Practice of Authentication, EUROCRYPT 1985, 261 (1986)	1986	Simmons II
Gustavus J. Simmons	G. Simmons, Contemporary Cryptography: The Science of Information Integrity, IEEE Press (1992).	1992	Simmons III
Karen R. Sollins	K.R. Sollins, Cascaded Authentication, Proceedings of the 1988 IEEE Conference on Security and Privacy (1988)	1988	Sollins
Ph. van Heurc	Ph. van Heurck, TRASEC: National Security System for EFTs in Belgium, Smart Card 2000 109-23 (D. Chaum ed., Elsevier Science Publishers B.V.) (1991)	1991	TRASEC '91
Ph. van Heurck	Ph. van Heurck, TRASEC: National Security System of EFTs in Belgium, 14 Computer Networks and ISDN Systems 389 (1988)	1988	TRASEC '88

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Stephen B. Weinstein	S. Weinstein, Emerging Telecommunications Needs of the Card Industry, 22 IEEE Communications Magazine 26 (July 1984)	1984	Weinstein
Karl Rihaczek	Karl Rihaczek, "OSIS Open Shops for Information Services," Computer Compacts, Vol. 1, Issue 3, pp. 136-44 (June 1983)	1983	Rihaczek Article
American National Standards Institute, Inc.	"American National Standard for Business Data Interchange – Invoice Transaction Set (810)," ANSI X12.2-1983	1983	ANSI 1983
American National Standards Institute, Inc.	"American National Standard for Business Data Interchange – Invoice Transaction Set (810)," ANSI X12.2-1986	1986	ANSI 1986
Houghton Mifflin Company	The American Heritage Dictionary of the English Language, Houghton Mifflin Company, p. 689 (1981)	1981	American Heritage Dictionary
Jan Ekberg	Jan Ekberg, "Tietosuojan Tulevaisuudennäkymiä," Sahko Electricity in Finland, Vol. 58, Pt. 5, pp. 30-36, 53 (1985)	1985	Ekberg
Sead Muftic	Sead Muftic, Security Mechanisms for Computer Networks, Ellis Horwood Limited (1989)	1989	Muftic Book
Dorothy E. Denning & Giovanni Maria Sacco	Dorothy E. Denning & Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, No. 8 (1981)	1981	Denning Article
Dorothy Elizabeth Robling Denning	Dorothy Elizabeth Robling Denning, Cryptography and Data Security, Addison-Wesley Publishing Co. (1982)	1981	Denning Book
Luc Longpre	Luc Longpre, "The Use of Public-Key Cryptography for Signing Checks," Proceedings of Crypto '82, pp. 187-97	1982	Longpre
Sead Muftic	Sead Muftic, "Secure Exchange of Sensitive Data in a Computer Network," Security and Protection in Information Systems, Elsevier Science Publishers (1989)	1989	Muftic Article

Primary Author or Publisher	Reference Title and Citation	Publication Date	Herein Referenced As
Roger M. Needham & Michael D. Schroeder	Roger M. Needham & Michael D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, Vol. 21, No. 12, pp. 993-99 (1978)	1978	Needham
Weijun Wang & Tom Coffey	Weijun Wang & Tom Coffey, "Network Security: Design of a Global Secure Link," Proceedings of the IFIP TC11 Eighth International Conference on Information Security, IFIP/Sec '92, Singapore, 27-29 May 1992	1992	Wang
Ronald Ferreira, Bruno Michaud & Jean-Jacques Quisquater	Ferreira, Michaud & Quisquater, "Key Management Protocols Using Smart Card," Proceedings of the IFIP WG 11.6 International Conference on SMART CARD 2000: The Future of IC Cards, Laxenaburg, Austria, October 19-20, 1987	1989	Ferreira
Dal Hyeoung Bae	Dal Hyeoung Bae, "Internal Control in an EDI Environment," M.S. Thesis, Naval Postgraduate School	1991	Bae
Daniel Drake, John Ciucci & Ben Milbrandt	Drake, Ciucci & Milbrandt, "Electronic Data Interchange in Procurement," Report PL904R1, Logistics Management Institute, Bethesda, Maryland	1990	Drake
Amir Herzberg & Shlomit Pinter	Herzberg & Pinter, "Public Protection of Software," ACM Transactions on Computer Systems, Vol. 5, No. 4, pp. 371-393	1987	Herzberg
Danny Cohen	Cohen, "Electronic Commerce," ISI Research Report ISI/RR-89-244, October 1989, Information Sciences Institute, University of Southern California	1989	Cohen
W. Michael Bridges and Bruce Kaplan	Bridges & Kaplan, "Implementation of Electronic Funds Transfer for Transportation Vendor Payment," Report PL005R2, Logistics Management Institute, Bethesda, Maryland	1992	Bridges

The above list is not exclusive or exhaustive, and MasterCard may rely on additional references that render one or more of the Asserted Claims invalid. MasterCard also reserves the right to rely on other art that may become known and/or relevant during the course of this litigation.

B. Disclosure Of Invalidity Due to Anticipation or Obviousness

1. Prior Art that Anticipates the Asserted Claims

Pursuant to the Patent Pretrial Order, ¶ I(2)(b), prior art references anticipating some or all of the Asserted Claims are listed below in Table 3. A full citation to each reference is found in Tables 1 and 2, along with the "Short Name" used to identify each reference throughout these disclosures, including in the claim charts. The Tables identify the claims anticipated by each reference and identify specific examples of where each limitation of the anticipated claims is found in that reference. MasterCard offers its invalidity contentions in response to Stambler's Infringement Contentions and without prejudice to any position they may ultimately take as to any claim construction issues.

Depending on the Court's construction of the claims of the '302 patent, and/or positions that Stambler or its expert witness(es) may take concerning claim interpretation, infringement, and/or invalidity issues, different combinations of the charted references may be implicated. Given this uncertainty, the charts may reflect alternative applications of the prior art against the Asserted Claims. The art cited in the charts is illustrative and not exhaustive. Though these claim charts provide illustrative citations to where each element may be found in the prior art references, the cited references may contain other disclosures of each claim element as well, and MasterCard reserves the right to argue that claim elements of the Asserted Claims are disclosed in non- cited portions of these references.

Table 3: References Anticipating/ Rendering Obvious Claims of the ’302 Patent

Exhibit A Chart	Prior Art	Claims
Chart A1	DAVIES I	All asserted claims
Chart A2	DAVIES II	All asserted claims
Chart A3	X9.9-1986	All asserted claims
Chart A4	TRASEC ‘91	All asserted claims
Chart A5	EP ATALLA	All asserted claims
Chart A6	WHITE	All asserted claims
Chart A7	FISCHER ’877	All asserted claims
Chart A8	US ATALLA	All asserted claims
Chart A9	FIFIELD	All asserted claims
Chart A10	The RSA Public Key Cryptosystem (“RSA”), as publicly known and used (including without limitation as described, *e.g.*, in Rivest Paper, Rivest MD4, Rivest ’829, InfoWorld, and ComputerWorld.	All asserted claims
Chart A11	SHAIN	51, 53, 55
Chart A12	Baum-1991	All asserted claims
Chart A13	Matyas 1982	All asserted claims
Chart A14	BAI	All asserted claims
Chart A15	Brachtl 050	All asserted claims
Chart A16	Kerberos	All asserted claims
Chart A17	EDI	All asserted claims
Chart A18	Rosen	All asserted claims
Chart A19	Longpre	All asserted claims
Chart A20	Rihaczek Article	All asserted claims

Exhibit A Chart	Prior Art	Claims
Chart A21	Beutelspacher Article	All asserted claims

2. Prior Art Renders The Asserted Claims Obvious

To the extent any Asserted Claim is not rendered invalid on anticipatory grounds, the following prior art references, as well as the combinations described in Exhibit A, render obvious the claims listed below. These combinations are not exclusive, and MasterCard reserves the right to supplement and/or amend the obviousness arguments listed below, using any references listed in Tables 1 and 2 and any references that may become known to MasterCard during the course of discovery.

- Davies I, combined with Nechvatal, renders obvious claims 51, 53 and 55 of the ’302 patent.
- Davies I, combined with Fischer and Piosenka, renders obvious claim 56 of the ’302 patent.
- Davies I, combined with Rihaczek Article, renders obvious claims 53 and 56 of the ’302 patent.
- Davies II, combined with Rihaczek Article, renders obvious claims 53 and 56 of the ’302 patent.
- X9.9-1986, combined with X.509, renders obvious claim 56 of the ’302 patent.
- X9.9-1986, combined with Davies I, renders obvious claims 55 and 56 of the ‘302 patent.
- Fischer ‘877, combined with X9.9-1986, renders obvious claims 51, 53, 55 and 56 of the ’302 patent.
- Fifield, combined with Davies I, renders obvious claims 55 and 56 of the ’302 patent.

- Baum-1991, combined with X9.9-1986, Davies I, or X.509, renders obvious claims 51, 53 55, and 56 of the ’302 patent.
- Davies I, combined with the Rivest Paper, renders obvious claims 51, 53 55, and 56 of the ’302 patent.
- Matyas 1982, combined with the Rivest Paper, renders obvious claims 51, 53 55, and 56 of the ’302 patent.
- Kerberos, combined with Wagner, Rosen, or Neuman, renders obvious claims 51 and 56 of the ’302 patent.
- BAI, combined with X.509, renders obvious claim 56 of the ’302 patent.
- BAI, combined with Davies I, renders obvious claims 55 and 56 of the ’302 patent.
- Brachtl ’050, combined with X.509, renders obvious claims 53, 55 and 56 of the ’302 patent.
- Brachtl ’050, combined with Davies I, renders obvious claims 53, 55, and 56 of the ’302 patent.
- X.509, combined with Davies I, Matyas 1982, or Byles, renders obvious claims 53 and 56 of the ’302 patent.
- Beutelspacher, combined with Davies I, renders obvious claim 55 of the ‘302 patent.
- RSA, combined with Davies I, renders obvious claims 51, 53, 55, and 56 of the ’302 patent.
- RSA, combined with Matyas 1982, renders obvious claims 51, 53, 55, and 56 of the ’302 patent.

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed, MasterCard reserves the right to rely on any other combination of

any prior art references disclosed herein. MasterCard further reserves the right to rely upon combinations disclosed within the prosecution history of the references cited herein. These obviousness combinations reflect MasterCard's current understanding of the potential scope of the claims that Stambler appears to be advocating and should not be seen as MasterCard's acquiescence to Stambler's interpretation of the patent claims.

To the extent a finder of fact finds that a limitation of a given claim was not disclosed by one of the references identified above, those claims are nevertheless unpatentable as obvious because the Asserted Claims contain nothing that constitutes patentable innovation. To the extent not anticipated, no Asserted Claim goes beyond combining familiar elements according to known methods to achieve predictable results or does more than choose between clear alternatives known to those of ordinary skill in the art.

MasterCard further believes that no showing of a specific motivation to combine the prior art references disclosed above and in Exhibit A is required, as each combination of art would have no unexpected results, and at most would simply represent a known alternative to one of ordinary skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1739-40 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test, instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 1742. Nevertheless, in addition to the information contained in the section immediately above and elsewhere in these contentions, MasterCard hereby identifies additional motivations and reasons to combine the cited art in the paragraphs below.

One or more combinations of the prior art references identified above would have been obvious because these references would have been combined using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or a teaching, suggestion, or motivation in the prior art generally. In addition, it would have been obvious to try combining the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field of endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. In addition, the combination of the prior art references identified above would have been obvious because the combination represents the known potential options with a reasonable expectation of success.

Additional evidence that there would have been a motivation to combine the prior art references identified above includes the interrelated teachings of multiple prior art references; the effects of demands known to the design community or present in the marketplace; the existence of a known problem for which there was an obvious solution encompassed by the Asserted Claims of the ’302 patent; the existence of a known need or problem in the field of the endeavor at the time of the invention(s); and the background knowledge that would have been possessed by a person having ordinary skill in the art. For example, the prior art references are directed to solving the same problem: providing secure electronic communication, including secure electronic funds transfers. Thus, a skilled artisan seeking to solve this problem of securing electronic communications, including electronic funds transfers, would look to these cited references in combination.

In addition, the motivation to combine the teachings of the prior art references disclosed herein is found in the references themselves and: (1) the nature of the problem being solved, (2) the express, implied and inherent teachings of the prior art, (3) the knowledge of persons of ordinary skill in the art, (4) the fact that the prior art is generally directed towards methods and systems for conducting business transactions in the 1980s or early 1990s, and/or (5) the predictable results obtained in combining the different elements of the prior art.

Any reference or combination of references that anticipates or makes obvious an asserted independent claim also makes obvious any Asserted Claim dependent from that independent claim because every limitation of each dependent claim was known by a person of ordinary skill at the time of the alleged invention, and it would have been obvious to combine those known limitations with the independent claims at least as a matter of common sense and routine work. Accordingly, MasterCard contends that each Asserted Claim would have been obvious not only from the combinations explicitly defined in these contentions, but also by any combination of references that renders obvious an Asserted Claim.

Numerous prior art references reflect common knowledge and the state of the prior art before the priority dates of the ’302 patent. As it would be unduly burdensome to create detailed claim charts for the thousands of invalidating combinations, such charts are not provided. For at least the reasons described above and below in the examples provided, as well as in the attached claim charts, it would have been obvious to one of ordinary skill in the art to combine any of a number of prior art references, including any combination of those identified in the charts, to meet the limitations of the Asserted Claims. As such, MasterCard’s inclusion of exemplary combinations, in view of the factors and motivations identified in the preceding paragraph, does not preclude MasterCard from identifying other invalidating combinations as appropriate.

Additional reasons to combine include[2]:

1. Davies I in view of Nechvatal

Davies I teaches that signatures may be generated by computing hash values on the transaction information as an intermediate step. Nechvatal provides rationale for using hash functions in this manner, which include, among others, an explanation that hash functions mitigate the effects of data expansion and lower bandwidth transmission that result from generating digital signatures. Hash functions therefore allow the signing entity in Davies I 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. It would be obvious for a person of ordinary skill in the art to combine the teachings of Davies I and Nechvatal to implement an electronic funds transfer system in which the transactions are authenticated by digital signatures, as taught by Davies I.

2. Davies I in Combination with Fischer and further in view of Piosenka

A person of ordinary skill in the art would be motivated to combine the teachings of Davies I with the teachings of Fischer for securing messages, end-to-end. In greater detail, Davies I teaches generation/application of a signature on a message that is sent by a sender to a recipient. Along with the message, the sender may send a certificate that includes the sender's public key.

Using a sender's public key that is obtained from the received certificate, the recipient is able to verify the message signature. Fischer, in describing the signature verification procedure, explicitly discloses that the recipient may authenticate the sender's public key itself before using

[2] Although MasterCard presents additional reasons to combine here, it also includes bases for determining obviousness in the attached Exhibits A1-A21.

the public key to verify the message signature. Specifically, according to Fischer's signature verification procedure, the sender's certificate includes a hierarchy of all certificates and signatures by higher authorities that validate the sender's certificate. The receiver preliminarily validates the sender's public key by verifying the signature on the sender's certificate using a higher authority's certificate that is included in the sender's certificate.

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 I, 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.

Piosenka describes that a user's request for access is denied if the signature on the user's credential cannot be validated. A person of ordinary skill in the art would be motivated to augment the verification of message signatures and public keys, as taught by the combination of Davies I and Fischer, with the denial of request upon failure to verify the user's credential, as taught by Piosenka. A recipient of a message, e.g., an electronic funds transfer message, verifies the message based on authenticating the sender's public key certificate and the message signature. If either the certificate signature or the message signature does not verify successfully, the recipient denies the transaction.

3. Davies I in Combination with Rihaczek Article

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Davies I with the Rihaczek Article. Davies I could be combined with the Rihaczek Article for at least the same reasons discussed above with respect to the combination of Davies II with the Rihaczek Article.

4. Davies II in Combination with Rihaczek Article

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Davies II with the Rihaczek Article. The electronic cheque in the Davies II reference has the following structure:

1	Bank identity	2	Bank public key
3	Expiry date	4	Signature of 1-3 by central bank
5	Customer identity	6	Customer public key
7	Expiry date	8	Signature of 5-7 by bank
9	Cheque sequence number	10	Transaction type
11	Amount of payment	12	Currency
13	Beneficiary identity	14	Description of payment
15	Date and time	16	Signature of 9-15 by customer

Figure 4

The OSIS cheque comes in three parts. The first one is used by the receiver to authenticate the bank; the second one to authenticate the issuer; the third one contains the cheque's message and information used for message authentication:

Part 1

- Bank identification (issuer of the token);
- Issuer bank public key (1);
- Date of expiry of that key;
- Signature of the above three items by the OSIS central bank.

Part 2

- Customer identification (account number);
- Customer public key (1; see explanatory notes before);
- Date of expiry of that key;
- Limit of guarantee by issuer bank;
- Signature of above four items by the issuer bank.

Part 3

- Message type (2);
- Issuer bank and customer identification (3);
- Amount and currency;
- Date and time, probably Greenwich Mean Time GMT (4);
- Serial number of message;
- Purpose of payment;
- Beneficiary identification (bank and account number) (5);
- Random filters (6);
- Signature of the above eight items by the customer.

The Rihaczek Article shows that the Customer Identification information includes an account number of the customer, and also shows that the Beneficiary Identification information includes an account number of the beneficiary. The Rihaczek Article also shows that the customer and the seller have bank accounts stored at banks and that their accounts are debited and credited, respectfully during a payment as follows:

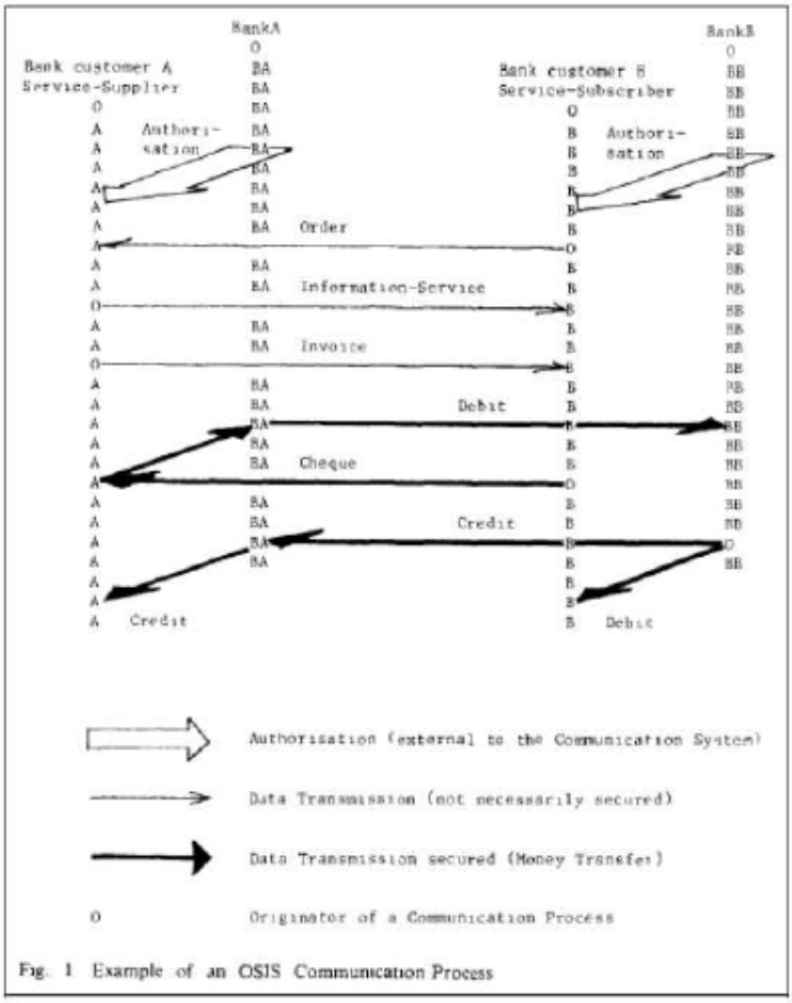

Fig. 1 Example of an OSIS Communication Process

One of ordinary skill in the art would have looked to the Rihaczek Article to see that the account information of the customer and the account information of the seller were stored at their banks, that the account information for the customer and seller were part of the information in the electronic cheque, and that the accounts were debited and credited as a result of the payment.

A motivation to combine exists because the Davies II reference and the Rihaczek Article are both directed to making payments with an almost identical electronic cheque, so the techniques of one would easily be used for the other.

5. X9.9-1986 in Combination with X.509

It would have been obvious to a person having ordinary skill in the art to combine the teachings of X9.9-1986 with X.509. One skilled in the art would have been motivated to combine the attributes of message authentication found in X9.9-1986 with the attributes of credentials in the form of certificates found in X.509, as both are taught in the context of security for electronic funds transfers ("EFTs"). Further, the similar use of the symmetric key cryptography to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine X9.9-1986 with X.509 and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of X9.9-1986 with those of X.509.

6. X9.9-1986 in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of X9.9-1986 with Davies I. One skilled in the art would have been motivated to combine the attributes of message authentication found in X9.9-1986 with the attributes of message authentication found in Davies I, as both are taught in the context of security for electronic funds transfers ("EFTs"). Further, the similar use of the Data Encryption Standard ("DES") algorithm to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine X9.9-1986 with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of X9.9-1986 with those of Davies I.

7. Fischer ’877 in Combination with X9.9-1986

It would have been obvious to a person having ordinary skill in the art to combine the teachings of X9.9-1986 with Fischer ’877. One having ordinary skill in the art would have been motivated to combine the attributes of message authentication found in X9.9-1986 with the digital signature certification of Fischer ’877, as both are taught in the context of security for electronic funds transfers (“EFTs”). Further, the similar use of the Data Encryption Standard (“DES”) algorithm to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine X9.9-1986 and Fischer ’877 and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of X9.9-1986 with those of Fischer ’877.

8. Fifield in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Fifield with Davies I. One skilled in the art would have been motivated to combine the attributes of message authentication found in Fifield with the attributes of message authentication found in Davies I, as both are taught in the context of security for EFTs. Further, the similar use of the Data Encryption Standard (“DES”) algorithm to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine Fifield with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Fifield with those of Davies I.

9. Baum-1991 in Combination with Davies I

It would have been obvious for a person having ordinary skill in the art to combine the teachings of Baum-1991 with Davies I. One skilled in the art would have been motivated to

combine the attributes of message authentication found in Baum-1991 with the attributes of error detection codes, credentials and public key encryption found in Davies I, as both are taught in the context of security for EFTs. Further, the similar use of the Data Encryption Standard ("DES") algorithm to secure information in EFTs would have increased the belief of a person of ordinary skill in the art that it would be sensible to combine Baum-1991 with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Baum-1991 with those of Davies I.

10. Baum-1991 in Combination with X.509

It would have been obvious for a person having ordinary skill in the art to combine the teachings of Baum-1991 with X.509. One skilled in the art would have been motivated to combine the attributes of message authentication found in BAUM 1991 with the attributes of certificates found in X.509, as both are taught in the context of security for EFTs. Further, the similar use of the public key cryptography to secure information in EFTs would have increased the belief of a person of ordinary skill in the art that it would be sensible to combine Baum-1991 with X.509 and that the combination would be successful. Further, one skilled in the art would have looked to X.509 as a relevant reference because Baum-1991 expressly discloses using X.509 digital certificates for public key infrastructure, distribution and authentication. X.509 was the industry-accepted standard for digital certificates and would have been well known to one of ordinary skill implementing a system, as in Baum-1991. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Baum-1991 with those of X.509.

11. Baum-1991 in Combination with X9.9-1986

It would have been obvious for a person having ordinary skill in the art to combine the teachings of Baum-1991 with X9.9-1986. One skilled in the art would have been motivated to

combine the attributes of using cryptographic algorithms (e.g. DES, RSA) to encrypt Electronic Data Interchange ("EDI") transactions and message authentication found in Baum-1991 with the attributes of using message authentication codes (MACs) for authenticating financial messages including electronic funds transfers, electronic financial messages with specific transaction information including the identity of the payor and payee, amount of the transfer and a description of the payment transaction and storage of originator/beneficiary account information at respective party's banks found in X9.9-1986 as both are taught in the context of security for EFTs. X.9.9-1986 was the industry-accepted standard for wholesale financial messaging, would have been well known to one of ordinary skill implementing a system as in Baum-1991 and, therefore, would have increased the belief of a person of ordinary skill in the art that it would be sensible to combine Baum-1991 with X9.9-1986 and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Baum-1991 with those of X9.9-1986.

12. Davies I in Combination with the Rivest Paper (Rivest '78)

It would have been obvious to a person having ordinary skill in the art to combine the teachings of the Rivest paper with Davies I, whose textbook makes multiple references to and uses of RSA work and teachings. One skilled in the art would have been motivated to combine the attributes of the bootstrap example found in the Rivest Paper with the electronic funds transfer ("EFT") techniques found in Davies I, as both are suggested for use in the EFT context. Moreover, a person having ordinary skill in the art would have been motivated to combine the bootstrap teachings of the Rivest Paper with the EFT systems of Davies I, because symmetric encryption was known to be faster, and public key encryption techniques were appreciated for their ability to send confidential data (such as a session key) that was digitally signed, as well as the role of a certificate authority (key distribution authority).

13. Matyas 1982 in Combination with the Rivest Paper (Rivest '78)

It would have been obvious to a person having ordinary skill in the art to combine the teachings of the Rivest Paper with those of Matyas and Meyer's textbook, which makes multiple uses of and references to RSA's work and teachings. One skilled in the art would have been motivated to combine the attributes of the bootstrap example found in the Rivest Paper with the EFT techniques found in Matyas, as both are suggested for use in the EFT context. Moreover, a person having ordinary skill in the art would have been motivated to combine the bootstrap teachings of the Rivest paper with the EFT systems described by Matyas, because symmetric encryption was known to be faster, and public key encryption techniques were appreciated for their ability to send confidential data (such as a session key) that was digitally signed, as well as the role of a certificate authority (key distribution authority). The Matyas reference itself discloses the use of session keys in end-to-end encryption in Chapter 4 at pp. 206-208. It would be well known to one of ordinary skill in the art in 1982 that the Xi,j data could include a session key and thus the method described by Matyas at p. 582 can cause a symmetric session key to be distributed to all parties in a communications using a public-key algorithm. Matyas discloses the form of communications from node i to node j in an asymmetric system as "EPKjDSKi(Xi,j) where Xi,j are the data sent from node i to node j whose integrity and secrecy must be maintained." (p. 582) It would be well known to one of ordinary skill in the art in 1982 that the Xi,j data could include a session key and thus the method described by Matyas at p. 582 can cause a symmetric session key to be distributed to all parties in a communications using a public-key algorithm. "The KDC could also be used with an asymmetric algorithm. In that case the KDC would store all n public keys and route them to the system nodes as required." (p. 583).

14. Kerberos in Combination with Wagner, Rosen, and/or Neuman

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Kerberos with Wagner, Rosen, and/or Neuman. For example, one having ordinary skill in the art would have been motivated to combine the security measures disclosed in Kerberos with the financial transactions of Wagner, such financial transactions inherently benefitting from security measures. Also, at least one of the architects of the Kerberos system recognized that Kerberos could be used to provide security and authentication in financial transactions. See, e.g., B. Clifford Neuman, "Proxy-Based Authorization and Accounting for Distributed Systems," Technical Report 91-02-01, March 1991 (describing the use of Kerberos in the context of banking and financial transactions and the benefits associated with its use). Accordingly, it would have been obvious to one of skill in the art to combine the teachings of Kerberos with the teachings of Wagner, Rosen, and/or Neuman in order to provide authentication and security in financial transactions.

15. BAI in Combination with X.509

It would have been obvious to a person having ordinary skill in the art to combine the teachings of BAI with X.509. For example, one skilled in the art would have been motivated to combine the attributes of message authentication found in BAI with the attributes of credentials in the form of certificates found in X.509, as both are taught in the context of security for electronic funds transfers ("EFTs"). Further, the similar use of the symmetric key cryptography to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine BAI with X.509 and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of BAI with those of X.509.

16. BAI in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of BAI with Davies I. For example, one skilled in the art would have been motivated to combine the attributes of message authentication found in BAI with the attributes of message authentication found in Davies I, as both are taught in the context of security for electronic funds transfers ("EFTs"). Further, the similar use of the Data Encryption Standard ("DES") algorithm to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine BAI with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of BAI with those of Davies I.

17. Brachtl '050 in Combination with X.509

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Brachtl '050 with X.509. For example, one skilled in the art would have been motivated to combine the attributes of message authentication found in Brachtl '050 with the attributes of credentials in the form of certificates found in X.509, as both are taught in the context of security for electronic funds transfers ("EFTs"). Further, the similar use of the symmetric key cryptography to secure information in EFTs would have demonstrated to and increased the belief of a person of ordinary skill in the art that it would be sensible to combine Brachtl '050 with X.509 and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Brachtl '050 with those of X.509.

18. Brachtl '050 in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Brachtl '050 with Davies I. For example, one skilled in the art would have been

motivated to combine the attributes of message authentication found in Brachtl ‘050 with the attributes of credentials and public key encryption found in Davies I, as both are taught in the context of security for EFTs. Further, the similar use of the Data Encryption Standard (“DES”) algorithm to secure information in EFTs would have increased the belief of a person of ordinary skill in the art that it would be sensible to combine Brachtl ’050 with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Brachtl ’050 with those of Davies I.

19. X.509 in Combination with Davies I, Matyas 1982, or Byles

It would have been obvious to a person having ordinary skill in the art to combine the teachings of X.509 with Davies I, Matyas 1982, or Byles. One skilled in the art would have been motivated to combine the EFT techniques disclosed in Davies I, Matyas 1982, or Byles with the attributes of credentials in the form of certificates found in X.509, as both are taught in the context of security for EFTs. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of X.509 with those of Davies I, Matyas 1982, or Byles.

20. Beutelspacher in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of Beutelspacher with Davies I. For example, one skilled in the art would have been motivated to combine the attributes of the certificates and message authentication found in Beutelspacher with the attributes of credentials found in Davies I, as both are taught in the context of security for smart cards and EFTs. Further, the similar use of the Data Encryption Standard (“DES”) algorithm to secure information in EFTs would have increased the belief of a person of ordinary skill in the art that it would be sensible to combine Beutelspacher with Davies I and that the combination would be successful. Thus, a person having ordinary skill in the art would have been motivated to combine the teachings of Beutelspacher with those of Davies I.

21. RSA in Combination with Davies I

It would have been obvious to a person having ordinary skill in the art to combine the teachings of RSA with Davies I, whose textbook makes multiple references to and uses of RSA work and teachings. One skilled in the art would have been motivated to combine the attributes of the bootstrap example found in RSA with the electronic funds transfer ("EFT") techniques found in Davies I, as both are suggested for use in the EFT context. Moreover, a person having ordinary skill in the art would have been motivated to combine the bootstrap teachings of RSA with the EFT systems of Davies I, because symmetric encryption was known to be faster, and public key encryption techniques were appreciated for their ability to send confidential data (such as a session key) that was digitally signed, as well as the role of a certificate authority (key distribution authority).

22. RSA in Combination with Matyas 1982

It would have been obvious to a person having ordinary skill in the art to combine the teachings of RSA with those of Matyas and Meyer's textbook, which makes multiple uses of and references to RSA's work and teachings. One skilled in the art would have been motivated to combine the attributes of the bootstrap example found in RSA with the EFT techniques found in Matyas, as both are suggested for use in the EFT context. Moreover, a person having ordinary skill in the art would have been motivated to combine the bootstrap teachings of RSA with the EFT systems described by Matyas, because symmetric encryption was known to be faster, and public key encryption techniques were appreciated for their ability to send confidential data (such as a session key) that was digitally signed, as well as the role of a certificate authority (key distribution authority). The Matyas reference itself discloses the use of session keys in end-to-end encryption in Chapter 4 at pp 206-208. It would be well known to one of ordinary skill in the art in 1982 that the Xi,j data could include a session key and thus the method described by

Matyas at p. 582 can cause a symmetric session key to be distributed to all parties in a communications using a public-key algorithm. Matyas discloses the form of communications from node i to node j in an asymmetric system as "EPKjDSKi(Xi,j) where Xi,j are the data sent from node i to node j whose integrity and secrecy must be maintained." (p. 582) It would be well known to one of ordinary skill in the art in 1982 that the Xi,j data could include a session key and thus the method described by Matyas at p. 582 can cause a symmetric session key to be distributed to all parties in a communications using a public-key algorithm. "The KDC could also be used with an asymmetric algorithm. In that case the KDC would store all n public keys and route them to the system nodes as required." (p. 583).

C. Contentions Under 35 U.S.C. § 101

The following contentions are subject to revision and amendment pursuant to Rule 26(e) of the Federal Rules of Civil Procedure and the Patent Pretrial Order to the extent appropriate in light of further investigation and discovery regarding the defenses, the Court's construction of the claims at issue, and/or the review and analysis of expert witnesses.

Failure To Claim Patentable Subject Matter Under *Bilski*. All of Stambler's Asserted Claims are invalid for failing to claim patentable subject matter under 35 U.S.C. § 101. *See, e.g., Bilski v. Kappos*, 130 S.Ct. 3218 (2010). Stambler's Asserted Claims are not patentable subject matter under 35 U.S.C. § 101 because the claims are method claims that consist of nothing more than abstract ideas. The Supreme Court held that if a patent seeks to claim an application of an abstract idea, it must contain an "inventive concept" sufficient to ensure that the patent in practice amounts to "significantly more" than a patent upon the abstract idea itself. *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294 (2012) (citations omitted). As useful and important evidence establishing the unpatenability of the Asserted Claims under §101, all of the claims fail to (1) involve a physical transformation or (2) be tied to a particular

physical apparatus or machine. *See Bilski v. Kappos*, 130 S.Ct. at 3221 (The Court holding that the Federal Circuit's machine-or-transformation test is not the sole criterion on which to determine patentability but remains a "useful and important clue" as an investigative tool in determining patentability under 35 U.S.C. § 101), *citing In re Bilski*, 545 F.3d 943, 960 (Fed. Cir. 2008) (*en banc*).

To meet the "transformation" prong of the machine-or-transformation test, a claim must transform a physical object or substance, or something representing a physical object or substance, into a different state or thing. *See Bilski*, 545 F.3d at 963. Claims that merely manipulate intangible information, like the Asserted Claims, fail the transformation prong of the machine-or-transformation test. *See Bilski*, 545 F.3d at 964. Stambler's claims do not involve a physical transformation required under the first prong of the machine-or-transformation test; rather, the claims merely manipulate information and at most merely manipulate *data* of a financial transaction. As recognized by the Federal Circuit, "[t]he mere manipulation or reorganization of data . . . does not satisfy the transformation prong." *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1375 (Fed. Cir. 2011).

Moreover, the Supreme Court has recently reinforced that merely requiring implementation by a generic computer fails to transform an abstract idea into a patent-eligible invention. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l, et al.*, No. 13-298 (U.S. June 19, 2014).

Further, by way of example, claim 51 of the '302 patent recites:

> 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.

Claim 51 merely manipulates data by reciting steps of "receiving funds transfer information," "generating a variable authentication number," "determining whether the at least a portion of the received funds transfer information is authentic," and "transferring funds." "Generating a variable authentication number" takes a set of data (received funds transfer information) and creates new data (a VAN). "Transferring funds," in the context of the patent at issue, relates to an originator's bank debiting the originator's account and then authorizing the recipient's bank to pay the check. (*See, e.g.*, '302 patent, col. 7, ll. 28-30). Therefore, claim 51 fails to recite a physical transformation. This is also true for all of the other Asserted Claims by Stambler, which all depend on claim 51—none of these claims involve a physical transformation. Further, the Asserted Claims fail to tie the claimed subject matter to a particular machine or apparatus. The Asserted Claims do not recite an apparatus at all, nor are they tied to any concrete parts, devices, or combination of devices. *See, e.g.*, '302 patent claims 51, 53, 55, and 56. Even assuming that the claims of the '302 patent implicitly require a computer, at most only a general purpose computer would be "required," which is incidental to the performance of the claimed method. This is insufficient to impose "meaningful limits" on the claim's scope. *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012).

Accordingly, Stambler's Asserted Claims are non-statutory subject matter and invalid under 35 U.S.C. § 101.

D. Contentions Under 35 U.S.C. § 112

The following contentions are subject to revision and amendment pursuant to Federal Rule of Civil Procedure 26(e) and the Court's Orders of record in this matter to the extent appropriate in light of further investigation and discovery regarding the defenses, the Court's construction of the claims at issue, and/or the review and analysis of expert witnesses.

To the extent the following contentions reflect constructions of claim limitations consistent with or implicit in Stambler's Infringement Contentions, no inference is intended nor should any be drawn that MasterCard agrees with Stambler's claim constructions, and MasterCard expressly reserves the right to contest such claim constructions. MasterCard offers such contentions in response to Stambler's Infringement Contentions and without prejudice to any position they may ultimately take as to any claim construction issues.

Subject to the reservation of rights above, MasterCard provides a chart attached as Exhibit B identifying the Asserted Claims and the specific limitations that fail to comply with 35 U.S.C. § 112 ¶ 1 (for lacking written description and/or enablement support) and/or 35 U.S.C. § 112 ¶ 2 (for indefiniteness). In addition, MasterCard provides below general contentions of invalidity pursuant to 35 U.S.C. § 112 ¶¶ 1 and 2.

To the extent an Asserted Claim is construed to cover an Internet-based payment system or method, the claims are invalid under 35 U.S.C. § 112, ¶¶ 1 and 2. The Stambler patents fail to adequately describe or enable claim coverage for Internet-based systems.

Lack of Enablement. The Asserted Claims are invalid because they do not enable one of ordinary skill in the art at the time the invention was made to make or use an invention as claimed. Moreover, the Asserted Claims as applied in Stambler's Amended Infringement Contentions are not supported by the specification of the '302 patent. Therefore, the Asserted Claims are invalid under 35 U.S.C. § 112 ¶ 1. In addition, to the extent the claims recite a

combination of method steps and other limitations, where the particular combination claimed was disclosed in the specification in a manner that teaches a person of ordinary skill in the art to make or carry out the claimed invention without undue experimentation, they are also invalid under 35 U.S.C. § 112, ¶ 1. Stambler fails to offer any method or system addressing the possibility of fraud by one party against the other, as noted in the prior art. *See, e.g.*, Davies II at 16.

Regards as the Invention. The Asserted Claims are invalid under 35 U.S.C. § 112, ¶ 2 to the extent the claims recite a combination of method steps and other limitations that do not particularly point out and distinctly claim the subject matter that the patent applicant regards as his invention.

Lack of Written Description. The Asserted Claims are invalid under 35 U.S.C. § 112, ¶ 1 to the extent the claims recite a combination of method steps and other limitations, where the particular combination claimed was not contemplated by or in possession of Stambler when the application was filed, or where any step or limitation of that combination is not disclosed in the patent application.

Indefiniteness Under § 112, ¶ 2. The Asserted Claims are invalid under 35 U.S.C. § 112, ¶ 2 for indefiniteness to the extent the claims purport to claim a method comprising a series of steps, but then positively recite one or more method steps in combination with a positively recited actor (human being or entity) for doing something or, as Stambler asserts in his Amended Infringement Contentions, a computer (server) for performing the claimed function.

Indefiniteness Under § 112, ¶ 6. The Asserted Claims are invalid under 35 U.S.C. § 112, ¶ 6 for indefiniteness to the extent the claims include a means plus function or step plus function limitation, but the patent's written description fails to disclose the claimed means or

step for performing the recited function or act and/or fails to clearly link disclosed structure or acts to performance of the recited function or act. To the extent an Asserted Claim includes a limitation under 35 U.S.C. § 112, ¶ 6, in which the associated act or structure involves a general purpose computer, but for which there is no, or insufficient, disclosure in the specification of the algorithms executed by the processor to accomplish the recited function or step, that claim is invalid for indefiniteness.

Dependent Claims. If any Asserted Claim is invalid for any reason under 35 U.S.C. § 112, all claims depending directly or indirectly therefrom are invalid for at least the same reasons. Accordingly, each of the asserted dependent claims incorporates by reference all § 112 invalidity contentions of the parent claims.

Dated: July 11, 2014

Respectfully submitted,

By: /s/ Robert C. Scheinfeld

Janet T. Munn, Fla. Bar No. 501281
Rasco Klock Perez Nieto
283 Catalonia Avenue, Suite 200
Coral Gables, Florida 33134
Telephone: 305.476.7101
Facsimile: 305.476.7102

Robert C. Scheinfeld, *pro hac vice*
Eliot D. Williams, *pro hac vice*
Christopher R. Patrick, *pro hac vice*
BAKER BOTTS L.L.P.
30 Rockefeller Plaza, 44th Floor
New York, New York 10112-4498
212/408-2500
212/408-2501 (Facsimile)

Attorneys for Defendants and Counterclaim Plaintiffs MasterCard Incorporated and MasterCard International Incorporated

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document is being served this the 11th day of July, 2014, on all counsel of record via electronic mail:

VIA ELECTRONIC MAIL

Joshua B. Spector, Esq.
jspector@phyalaw.com
Perlman, Bajandas, Yevoli & Albright, P.L.
1000 Brickell Avenue, Suite 600
Miami, Fl 33131
Telephone: 305.377.0086
Facsimile: 305.377.0781
Attorneys for Plaintiff Leon Stambler

Barry J. Bumgardner
barry@nbclaw.net
Edward R. Nelson, III
enelson@nbclaw.net
Nelson Bumgardner Casto, P.C.
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
Telephone: 817.377.9111
Facsimile: 817.377.3485
Attorneys for Plaintiff Leon Stambler

By: /s/ Robert C. Scheinfeld