Filed on behalf of Experian Marketing Solutions, Inc. and Epsilon Data Management, LLC

By: Kenneth J. Sheehan,
Lead Counsel
Registration No. 36,270
Shawnna M. Yashar,
Backup Counsel
Registration No. 59,624
BAKER & HOSTETLER LLP
Washington Square, Suite 1100
1050 Connecticut Avenue, NW
Washington, DC 20036-5304

By: Arthur Dresner, Lead Counsel
Registration No. 24,403
Jordana Garellek, Backup Counsel
Registration No. 67,859
DUANE MORRIS LLP
1540 Broadway
New York, NY 10036-4086

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Experian Marketing Solutions, Inc.
and
Epsilon Data Management, LLC
Petitioners
v.

RPost Communications Limited
Patent Owner

Patent No. 8,224,913
SYSTEM AND METHOD FOR VERIFYING DELIVERY AND INTEGRITY OF ELECTRONIC MESSAGES

PETITION FOR COVERED BUSINESS METHOD PATENT REVIEW UNDER 35 U.S.C. § 321 AND SECTION 18 OF THE LEAHY-SMITH AMERICA INVENTS ACT

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

Pursuant to 35 U.S.C. § 321, Section 18 of the Leahy-Smith America Invents Act ("AIA"), and 37 C.F.R. § 42.300 *et seq.*, the undersigned, on behalf of petitioners, Experian Marketing Solutions, Inc. and Epsilon Data Management LLC (collectively, "Petitioners"), hereby request a Covered Business Method post-grant review of claims 1-11 (all claims) of U.S. Patent No. 8,224,913 ("the '913 patent," attached as Exhibit 1001).

The '913 patent is directed to a method and a system for electronic mail certification. The '913 patent discloses a "system and method for verifying delivery and content of an electronic message and . . . later providing proof regarding the delivery and content of an e-mail message." '913 patent at 1:20-25.

As known by anyone who used electronic email communication prior to 1999, verifying the delivery and content of an e-mail was well known in the industry. Clark Decl. at ¶ 31. As demonstrated below, while the '913 patent claims priority to 1999, multiple prior art publications taught in detail exactly what is claimed by the '913 patent. None of this prior art was disclosed or considered during prosecution of the '913 patent.

For the reasons set forth in this petition, claims 1-11 of the '913 patent are unpatentable, under 35 U.S.C. §§ 102 and/or 103, in view of the prior art publications cited herein. Petitioners, therefore, respectfully request review of

these claims under the transitional program for covered business method patents defined in 37 C.F.R. §42.300.

A. Overview of the ’913 Patent

The ’913 patent issued to Terrance A. Tomkow (“Tomkow”) from U.S. Pat. App. No. 12/952,076, filed on November 22, 2010 and claiming priority to U.S. Provisional App. Nos. 60/146,074 filed Jul. 28, 1999 and 60/172,479 filed Dec. 17, 1999. The ’913 patent is entitled “System And Method For Verifying Delivery And Integrity Of Electronic Messages.” The recorded assignments for the ’913 patent indicate that the ’913 patent is putatively owned by RPost Communications Limited, and putatively licensed exclusively to RPost Holdings, Inc. (collectively, RComm and RPH are referred to as “Patent Owner” or “RPost”). *See* Exhibit 1002.

The ’913 patent discloses a “system and method for verifying delivery and content of an electronic message and, more particularly, to a system and method of later providing proof regarding the delivery and content of an e-mail message.” ’913 patent at 1:20-25. The ’913 specification describes the invention as being “a system and method for reliably verifying via secure and tamper-proof documentation the content and delivery of an electronic message such as an e-mail” with the desired purposes of giving “e-mail and other electronic messages a legal status on a par with, if not superior to, that of registered United States mail.” ’913 patent at 3:6-11. In order to generate this “proof regarding the delivery and

content of an e-mail message," the '913 specification requires, and the claims expressly recite, using a third-party Mail Transport Agent (MTA) that records at least a portion of the SMTP (or ESMTP). *See, e.g.*, '913 patent at Fig. 1; 6:39-50; 11:40-12:2; Fig. 8; and 24:60-25:31.

This third-party MTA is essential to the invention claimed in the '913 patent. In the DESCRIPTION OF THE RELATED ART section, the '913 specification disclaimed the return-receipt methods known in the prior art that do not require using a third-party MTA:

> Many existing e-mail systems and e-mail programs already provide for some form of proof of delivery. For instance, some e-mail systems today allow a sender to mark a message with 'request for notifications' tags. Such tags allow a sender to request notification that the message was delivered and/or when the message was opened. . . . "[h]owever, this does not mean that an e-mail sent with a notification request is as effective in all respects as registered mail.

'913 patent at 1:43-67. The use of the third-third party MTA was seen by the applicant to be a necessary component in order to "provide reliable proof of the content and delivery of electronic messages" without "compliance of co-operation of the recipient" and "which requires no special e-mail software on the part of the sender or recipient." '913 patent at 2:65-3:1.

The '913 patent teaches using the MTA to relay the sender's message to the recipient, while maintaining a record of the SMTP (or ESMTP) dialog between the

MTA and the recipient as proof of the recipient's receipt. *See, e.g.*, '913 patent at Fig. 1; 6:39-50; 7:1-33; 8:4-8; 10:36-53 and claim 1 ("transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent.").

The '913 specification further recites that "[t]he present invention includes an electronic message system that creates and records a digital signature of each electronic message sent through the system." '913 patent 3:18-20. However, the '913 specification clarifies that creating the digital signature is not innovative: "The digital signature can be created using known digital signature techniques, such as by performing a hash function on the message to produce a message digest and then encrypting the message digest." '913 patent at 3:55-58.

B. The Prosecution History of the '913 Patent

In a non-final Office Action dated June 9, 2011, the Examiner rejected the claims under 35 U.S.C. 102(e) as being anticipated by Liu et al, U.S. Pat. No. 6,760,752, as well as under 35 U.S.C. 103(a) as being unpatentable over Liu in view of "Network Design Manual: Storing and Forwarding With SMTP and Message Transfer Agents," Feb 23, 1999. *See* Ex. 1003 at 1003.161-167.

In order to place the application in a condition for allowance, the applicant argued in an Amendment dated December 9, 2011 as follows:

> Claim 29 was amended, among other amendments, to recite ***recording*** at the server some portion of the SMTP and ESMTP protocol dialog between the server and recipient, including portions in which the

> receiving Mail Transport Agent of the recipient accepts or declines delivery of the transmitted message. . . . Liu et al. discloses an email system that uses various encryption methods and public and private keys. Information is passed back and forth between senders and recipients. However, ***nowhere does Liu et al. teach or suggest recording some portion of a mail transport protocol dialog generated during transmission*** of the message between the server and Mail Transport Agent for a recipient, as is claimed in amended claim 29.

Ex. 1003 at 1003.151. In response to that same Office Action, the applicant also argued that:

> Moreover, while Liu et al does teach using conventional network communication protocols such as HTTP, SMTP and the like to transmit electronic documents, Liu et al. does not teach or suggest ***storing some portion of the dialog*** generated by those protocols during transmission of the document from the server to a Mail Transport Agent of the recipient, as is claimed in amended claim 29. ***Using a protocol to communicate documents in a network is not the same as recording some portion of the communications*** between servers and destinations that occur as the result of using that protocol. While persons skilled in the art would have been aware of the flow of information that is part of the protocol, ***Applicant alone recognized the importance of storing the dialog that occurs between a server and destination address that is generated when using a mail transport protocol such as SMTP for later use in proof of the message and proof of the delivery of the message.***

Ex. 1003 at 1003.150-151, Amendment dated December 9, 2011 (emphasis added).

These remarks demonstrate how the applicant distinguished the inventions claimed in the ’913 patent from the prior art by arguing that the “recording [and storing] at the server some portion of the selected one of the SMTP and ESMTP protocol dialog” limitation in independent claims 1 and 10 was a critical distinction between the prior art and the claimed inventions. It is important to note that claims 2-9, which are dependent on claim 1, and claim 11, which is dependent on claim 10, were allowed because they depend on a claim reciting the “recording” limitation. The dependent claims do not add any subject matter that could be used to distinguish the ’913 patent from the prior art.

II. MANDATORY NOTICES (37 C.F.R. § 42.8)

The Real Parties-in-Interest (37 C.F.R. § 42.8(b)(1)) are Experian Marketing Solutions, Inc. and Epsilon Data Management, LLC (“Petitioners”). As of the filing date of the petition, the ’913 patent was asserted against the parties-in-interest in *RPost Holdings, Inc. v. Epsilon Data Management*, LLC, E.D. Tex. No. 2:12-cv-00511-JRG and *RPost Holdings, Inc. v. Experian Marketing Solutions, Inc.*, E.D. Tex. No. 2:12-cv-00513-JRG (consolidated with -00511).

Petitioners are aware of the following pending judicial matters in which the Patentees have asserted the '913 patent that could affect, or be affected by, a decision in this proceeding (37 C.F.R. § 42.8(b)(2)):

- *RPost Holdings, Inc. v. Epsilon Data Management*, LLC, E.D. Tex. No. 2:12-cv-00511-JRG;
- *RPost Holdings, Inc. v. Experian Marketing Solutions, Inc.*, E.D. Tex. No. 2:12-cv-00513-JRG (consolidated with -00511);
- *RPost Holdings, Inc. v. Vocus, Inc.*, E.D. Tex. No. 2:12-cv-00516-JRG (consolidated with -00511);
- *RPost Holdings, Inc. v. Constant Contact, Inc.*, E.D. Tex. No. 2:12-cv-00510-JRG;
- *RPost Holdings, Inc. v. Strongmail Systems, Inc.*, E.D. Tex. No. 2:12-cv-00515-JRG;
- *RPost Holdings, Inc. v. Infogroup, Inc.*, E.D. Tex. No. 2:12-cv-00517-JRG; and
- *RPost Holdings, Inc. v. Docusign, Inc.*, E.D. Tex. No. 2:12-cv-00683-JRG.

Lead Counsel and Backup Counsel for Experian (37 C.F.R. § 42.8(b)(3)) are Kenneth J. Sheehan and Shawnna M. Yashar, respectively, both of BAKER & HOSTETLER LLP, 1050 Connecticut Ave. NW, Washington Square, Ste. 1100, Washington, DC 20036, phone 202.861.1500, facsimile 202.861.1783.

Epsilon identifies Arthur Dresner as lead counsel and Jordana Garellek and Jarrad Gunther as back-up counsel:

Arthur Dresner, Reg. No. 24,403
Lead Counsel
Jordana Garellek, Reg. No. 67,859

Jarrad M. Gunther, Reg. No. 63,903
Back-up Counsel
Duane Morris LLP

Back-up Counsel
Duane Morris LLP
1540 Broadway
New York, NY 10036-4086
Telephone: (212) 692-1014
Facsimile: (212) 202-4904
Email: ADresner@duanemorris.com
Email: JGarellek@duanemorris.com

30 S. 17th Street
Philadelphia, PA 19103
Telephone: (215) 979-1000
Facsimile: (215) 979-1020
Email: JMGunther@duanemorris.com

For service (37 C.F.R. §42.8(b)(4)) please direct all correspondence to backup counsel at the above address. Petitioners consent to e-mail service at ksheehan@bakerlaw.com, syashar@bakerlaw.com, ADresner@duanemorris.com, JGarellek@duanemorris.com, and JMGunther@duanemorris.com.

III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))

A. At Least One Challenged Claim is Not Patentable

As further detailed below, claims 1-11 (all claims) of the '913 patent are unpatentable under one or more of 35 U.S.C. §§ 102 and/or 103. Post-grant review is therefore warranted. *See* 35 U.S.C. § 324(a).

B. The '913 Patent is a Covered Business Method Patent

The '913 patent is a "covered business method patent" ("CBM") under § 18(d)(1) of the Leahy-Smith America Invents Act, Pub. L. 112-29 ("AIA") and 37 C.F.R. § 42.301. A CBM 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." 37 C.F.R. § 42.301. The scope of the CBM program has been refined by the USPTO's

rulemaking process. In particular, the USPTO has taken the position that a "financial product or service" should be "interpreted broadly" in view of the "legislative intent and history behind the public law definition [of that phrase] and the transitional program itself." Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention; Final Rule, 77 Fed. Reg. 48,734 (Aug. 14, 2012) at 48,735; *see also id.* at 48,734-35 (explaining that "the definition of covered business method patent was drafted to encompass patents 'claiming activities that are financial in nature, incidental to a financial activity or complementary to a financial activity") (citation omitted).

During the March 2011 debates on the AIA, Senator Schumer addressed the first element of the "financial services" part of the "covered business-method patent" definition and noted that:

> The amendment covers not only financial products and services, but also the "practice, administration and management" of a financial product or service. This language is intended to make clear that the scope of patents eligible for review under this program is not limited to patents covering a specific financial product or service. In addition to patents covering a financial product or service, the "practice, administration and management" language is intended to cover ***any ancillary activities related to a financial product or service***, including . . . marketing, customer interfaces, Web site management and

> functionality, transmission or management of data, servicing, underwriting, customer communications, and back office operations—*e.g.*, payment processing, stock clearing.

See 157 Cong. Rec. S1364–65 (daily ed. Mar. 8, 2011) (statement of Sen. Schumer) (emphasis added). Later, during the September 2011 debates, Senator Schumer further clarified that "[s]ection 18 does not restrict itself to being used by petitioners whose primary business is financial products or services. Rather, it applies to patents that can apply to financial products or services." *Id.* at S5432 (daily ed. Sept. 8, 2011) (statement of Sen. Schumer).

The '913 patent specification makes clear that the claimed electronic messaging system and methods are directed to financial, monetary, and commercial applications. Specifically, there are several *express* statements in the '913 patent specification directed to financial or monetary transactions, including:

- "This evidence can be presented any time a dispute arises regarding the content and delivery of messages, as for example in contract formation, ***the timing of stock buy or sell orders***, and many other applications." *Id.* at 17:46-49 (emphasis added);
- "In addition to the ***revenue sources*** available in other embodiments, in this embodiment the operators can ***charge storage fees*** for receipts held in the web based mailbox." *Id.* at 23:35-37 (emphasis added); and

- "The registered queries, complaints, ***orders, offers to purchase***, and other information 46 are sent to the e-business 30 by the system. Receipts are then provided to the customers 34 via SMPT server 38." *Id.* at 26:36-39 (emphasis added).

The USPTO has specified that additional guidance regarding the scope of the CBM Program should come from decisions on petitions as the PTAB makes them. *See* 77 Fed. Reg. at 48,737. In clarifying which patents qualify for CBM review, the PTAB has found that the term "financial product or service" should include patents claiming activities that are "complementary to a financial activity" and activities that "relate to monetary matters." *SAP Am., Inc. v. Versata Dev. Group, Inc.*, CBM2012-00001, Doc. 36 at 23 (stating that "[t]he term *financial* is an adjective that simply means relating to *monetary matters*") *Id.* (emphasis added).

The '913 patent relates to monetary matters. For instance, the '913 specification describes the invention as being an e-mail system used in "e-commerce." *Id.* at 3:42-46 ("For corporate or e-commerce users, these users can change their server to a server incorporating the present invention and have all of their external electronic messages registered, with the option of having the system retain and archive the receipts."). E-Commerce or the Electronic Commerce industry is defined as a type of industry where the buying and selling of products or services is conducted over electronic systems such as the Internet and other

computer networks. E-Commerce, like all commerce, revolves around commerce transactions which involve money.

To make these transactions possible, e-commerce necessarily draws on technologies such as mobile commerce, electronic funds transfer, on-line transaction processing, and electronic data interchange (EDI). *See*, Encyclopedia Britannica, *E-Commerce,* attached as Exhibit 1004 (defining e-commerce as encompassing "secure electronic transfer of sensitive information (such as credit card numbers and electronic funds transfer [EFT] orders)"). Consequently, e-commerce transactions represent exactly the type of activities that are "complementary to a financial activity" and "relate to monetary matters," as supported by precedent, the USPTO rulemaking commentary, and the legislative history behind the AIA. *See, e.g.*, *SAP v. Versata*, CBM2012-00001, Doc. 36 at 23; 77 Fed. Reg. at 48,734-35; and 157 Cong. Rec. at S1364-65.

More support for the '913 patent being the exact type of patent contemplated for CBM review can be found by looking at the claims themselves. Claims 5, 6, 8, 9 and 10 of the '913 patent require the use of "encryption" which the '913 patent specifications describes as being valuable in the e-commerce and financial industries because it is used to provide proof that "an order [has been] placed." '913 patent at 2:4. The specification goes on to explain that proof of delivery of a

message is necessary in cases "where acknowledging receipt of the message would place a financial or legal burden on the recipient." *Id*. at 2:40-42.

As noted in the legislative history of the AIA, Section 18 grew out of concerns regarding the Ballard patents which related to encryption technologies used to process checks electronically.

> This section grew out of concerns originally raised in the 110th Congress about financial institutions' inability to take advantage of the authority to clear checks electronically . . . without infringing the so-called Ballard patents, patents number 5,910,988 and 6,032,137 . . . Once the committee began to examine this issue in greater depth, however, the question quickly turned . . . to how it is that the Ballard patents were issued in the first place. These patents consist of long recitations of technology created by others to implement the supposed "invention" of transmitting and processing checks and other business records electronically. The first of these patents was assigned to the class of cryptography inventions, but its specification itself concedes that the invention's ''controller" will ''execute[] an encryption algorithm which is well known to an artisan of ordinary skill in the field.

157 Cong. Rec. S1379 (daily ed. Mar. 8, 2011) (statement of Mr. Kyl). Just like the patents that sparked the debate in the AIA, which lead to the eventual inclusions of the CBM program, the '913 patent uses well known encryption algorithms in the transmission of an electronic transaction (an e-mail) used to conduct business.

To make a determination of whether a patent qualifies as a CBM patent, the AIA's legislative history also instructs that the PTAB "may look to how the patent has been asserted." *Id.* The Patent Owner has made several public statements indicating that its patent portfolio, including the '913 patent, is directed to financial services. For example, the Patent Owner has a page on its website that specifically discusses how its registered email services are used in the "financial sector," including for "financial advisory/private client services," "investment banking," "trading operations," and "commercial banking." *See* Registered Email for Financial Services, *available at* http://www.rpost.com/industries/financial-services (last visited Oct. 4, 2013), attached as Exhibit 1005. Other pages on Patent Owner's website include similar statements:

- "A ***regional bank*** uses RPost's electronic signature services to record client signatures on contracts used to ***open new accounts*** for clients that are located internationally." *See* RPost Blog: Bank uses eSignOff services for international clients (Dec. 13, 2010), http://www.rpost.com/blog/548-bank-uses-esignoff-services-for-international-clients (emphasis added), attached as Exhibit 1006;

- "CertifiedEmail PS is Goodmail's premium service and is supposed to validate the exact contents of each email sent, with a date and time stamp confirming when it was sent and when it arrived in the recipient's server-level email inbox. ***It's targeted at banks, brokerage houses, credit card companies***, utilities,

insurance companies and healthcare concerns, the folks concerned with regulatory compliance." *See*, ePostal Goodmail lawsuit – ePostalNews (Oct. 5, 2009), http://www.rpost.com/news-and-events/press-room/media-coverage/341 (emphasis added), attached as Exhibit 1007; and

- "RPost's electronic signature services were used to record signoff on ***new sales contracts sent to international customers***." *See*, RPost Blog: RPost's electronic signature services used to record signoff on international sales contracts (Dec. 9, 2010), http://www.rpost.com/blog/543-rposts-electronic-signature-services-used-to-record-signoff-on-international-sales-contracts (emphasis added), attached as Exhibit 1008.

Because the '913 patent is directed towards the delivery and verification of e-mail through the use of encryption in e-commerce and the financial services industry, and because the Patent Owner is clearly marketing their patent portfolio as being directed towards the financial services industry, review under the CBM program is appropriate and respectfully requested.

C. The '913 Patent is Not Directed to a Technological Invention

The '913 patent is not exempt from review because it is not a technological invention. Patents for "technological inventions" are excluded from qualifying as CBM patents. AIA § 18(d)(2); *see also* 37 C.F.R. § 42.301. Whether a patent is directed to a "technological invention" is decided on a case-by-case basis and turns

on: (a) "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art;" and (b) "solves a technical problem using a technical solution." 37 C.F.R. § 42.301(b).

The '913 patent does not recite any novel and unobvious technological feature, and does not solve a technical problem. The Patent Office Trial Practice Guide ("Trial Guide") states that the "mere recitation of known technologies, such as computer hardware, communication or computer networks, software, memory, [and] computer-readable storage medium" "would not typically render a patent a technological invention." Trial Guide at 36; *see also Interthinx, Inc. v. CoreLogic Solutions, LLC*, CBM2012-00007, Doc. 15 at 18 (Jan. 31, 2013). The same is true for patents that "[r]ecite[] the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious." Trial Guide at 37.

The '913 patent specification admits that e-mail communication and authentication is not novel: "Many existing e-mail systems and e-mail programs already provide for some form of proof of delivery." '913 patent at 1:43-45. As discussed above, in order to place the application in a condition for allowance, the applicant (i) amended the independent claims to include the "recording" limitation; and (ii) argued that the prior art does not teach that limitation. *See, e.g.*, Ex. 1003 at 1003.151-152, ("[N]owhere does Liu et al. teach or suggest recording some portion

of a mail transport protocol dialog generated during transmission of the message between the server and Mail Transport Agent for a recipient, as is claimed in amended claim 29.").

None of the steps of claim 1 of "transmitting," "recording," or "accept[ing] or declin[ning] delivery of the transmitted message" require any novel and unobvious technological implementation or solve a technical problem. The same argument is applicable to the additional non-limiting elements of claim 10 of "calculating a digital digest," "encrypting the digital digest," "writing the encrypted digital digest," and "transmitting the message and the file to a recipient." Moreover, the '913 patent specification admits that "[t]he digital signature can be created using known digital signature techniques, such as by performing a hash function on the message to produce a message digest and then encrypting the message digest." '913 patent at 3:55-58.

In summary, the claims of the '913 patent merely recite using well-known technology (e-mail), in a well-known manner (using SMTP or ESMTP to transmit e-mail), to perform a well-known task (applying digital signatures). The '913 patent thus does not claim any technological invention, and it is not exempt from the definition of a CBM patent.

D. Petitioners Have Been Sued for Infringement and Are Not Estopped (37 C.F.R. § 42.302)

"A party sued for infringement of a patent, and not otherwise estopped from challenging validity, may file a [CBM] petition." *SAP*, CBM2012-000001, Doc. 36 at 18 (citing 37 C.F.R. § 42.302). Both requirements are met here.

The Patent Owner's complaints in *RPost Holdings, Inc. v. Epsilon Data Management*, LLC, E.D. Tex. No. 2:12-cv-00511-JRG and *RPost Holdings, Inc. v. Experian Marketing Solutions, Inc.*, E.D. Tex. No. 2:12-cv-00513-JRG (consolidated with -00511) assert the '913 patent against Petitioners. *See* Exhibits 1009 and 1010. Petitioners certify that they are not estopped by any final written order from challenging the claims on the grounds identified.

IV. PERSON OF SKILL IN THE ART DEFINITION

A person of skill in the art is one who is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity. Considering these factors in the context of the claims of the '913 patent, a person skilled in the art in the 1999 time frame would have a master's degree in computer science and two years of experience related to security and cryptography, or the equivalent. *See, e.g.*, Clark Decl. at ¶¶ 1-8 and 13.

V. STATEMENT OF PRECISE RELIEF REQUESTED FOR EACH CLAIM CHALLENGED (37 C.F.R. § 42.22(A))

A. Review is Requested for All Claims (37 C.F.R. § 42.304(b)(1))

Petitioners respectfully request review under 35 U.S.C. §321 and AIA §18 of claims 1-11 (all claims) of the '913 patent and cancellation of those claims on the grounds set forth below.

B. Statutory Grounds of Challenge (37 C.F.R. § 42.304(b)(2))

As further detailed below, claims 1-11 (all claims) of the '913 patent are being challenged as unpatentable under 35 U.S.C. §§ 102 and/or 103, as follows:

- Claims 1-11: Anticipated under 35 U.S.C. § 102 over Certified Exchange of Electronic Mail (CEEM) (Exhibit 1012**)**;
- Claims 1-9: Anticipated under 35 U.S.C. § 102 over Certified Electronic Mail (CEM) (Exhibit 1013**)**;
- Claims 10-11: Rendered obvious under 35 U.S.C. § 103 over Electronic Mail (CEM) (Exhibit 1013**)** in view of PEM (Exhibit 1014**)**; and/or
- Claims 1-3: Anticipated under 35 U.S.C. § 102 over Postfix **(**Exhibit 1016**)**.

C. Claim Construction (37 C.F.R. § 42.304(b)(3))

1. Broadest reasonable interpretation

A claim subject to CBM review receives the "broadest reasonable interpretation" ("BRI") in light of the specification. 37 C.F.R. § 42.300(b); *SAP*, CBM2012-00001, Doc. 36 at 6. The Board "begin[s] [its] analysis with the plain language of the claims themselves but look[s] to the specification for guidance as to how one skilled in the art would understand the ordinary meaning of the claims." *SAP* at 6. Care must be exercised in claim interpretation, as "there is a fine line between interpreting claims in light of the specification and reading limitations into the claims from the specification." *Id*.

"A claim's preamble may limit the claim when the claim drafter uses the preamble to define the subject matter of the claim." *August Tech. Corp. v. Camtek, Ltd*., 655 F.3d 1278, 1284 (Fed. Cir. 2011). Patent preambles are limiting when they are "necessary to give life, meaning and vitality to the claim" based "on the facts of the case at hand and in view of the claimed invention as a whole." *Allen Eng'g Corp. v. Bartell Indus*., 299 F.3d 1336, 1346 (Fed. Cir. 2002) (internal citations omitted). A preamble constitutes a limitation "when reciting additional structure . . . underscored as important by the specification." *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808-09 (Fed. Cir. 2002).

The doctrine of prosecution history estoppel prevents an applicant from making arguments during prosecution to overcome a prior art reference and then later seeking to broaden the claims to include the disclaimed material. *Seachange Int'l, Inc. v. C-COR, Inc.*, 413 F.3d 1361, 1372-73 (Fed. Cir. 2005). "[B]y distinguishing the claimed invention over the prior art, an applicant is indicating what the claims do not cover." *Spectrum Int'l v. Sterlite Corp*., 164 F.3d 1372, 1378-79 (Fed. Cir. 1998) (quotations omitted). The "applicant's argument that a prior art reference is distinguishable on a particular ground can serve as a disclaimer of claim scope even if the applicant distinguishes the reference on other grounds as well." *Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1374 (Fed. Cir. 2007).

2. The '913 Claim Terms

The terms of the '913 patent that warrant and permit construction are discussed below. Terms not addressed below should be presumed to take their ordinary and customary meanings for purposes of this review only.

Claim Term	BRI	Support
A method of transmitting a message (and an attachment to the message) from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This preamble is limiting because it is "necessary to give life, meaning and vitality to the claim." *Allen Eng'g Corp.* v. *Bartell Indus*., 299 F.3d 1336, 1346 (Fed. Cir. 2002).	In order to generate "proof regarding the delivery and content of an e-mail message," the '913 specification requires, and the claims expressly recite, using a third-party Mail Transport Agent (MTA) that records at

[Claims 1 and 10]		least a portion of the SMTP (or ESMTP). *See, e.g.*, '913 patent at Fig. 1; 6:39-50; 11:40-12:2; Fig. 8; and 24:60-25:31; *see also, e.g.*, Ex. 1003 at 1003.150-151.
server acting as a Mail Transport Agent [Claims 1 and 10]	A "server acting as a Mail Transport Agent" is a server acting as a third party to relay a message from the sender to the intended recipient's Mail User Agent, and confirm delivery of the message.	*See, e.g.*, '913 patent at Fig. 1; 2:24-40; 2:64-3:5; 6:39-50; 7:12-16; *see also* Clark Decl. at ¶ 32.

1. The Preambles Are Limiting

As discussed above, patent preambles are limiting when they are "necessary to give life, meaning and vitality to the claim" based "on the facts of the case at hand and in view of the claimed invention as a whole." *Allen Eng'g Corp.*, 299 F.3d at 1346. The preambles in independent claims 1 and 10 require the use of a server acting as a Mail Transport Agent to transmit the e-mail messages, with or without attachments. During prosecution, the applicant specifically argued that the prior art did not teach the claimed inventions because it did not suggest "recording some portion of a mail transport protocol dialog generated during transmission of the message between the server and Mail Transport Agent," nor did the prior art teach "storing some portion of the dialog generated by those protocols during the transmission of the document from the server to a Mail Transport Agent." Ex. 1003

at 1003.150-151. Moreover, the Applicant even acknowledged specifically amending the claims to recite "recording at the server some portion of the SMTP and ESMTP protocol dialog," which includes "portions in which the receiving Mail Transport Agent of the recipient accepts or declines delivery of the transmitted message." *Id*.

For at least this reason, the existence of a server acting as a Mail Transport Agent is clearly not just a preferred embodiment of the invention—it is a necessary structure. The inventions, as claimed, cannot be practiced without a server acting as an MTA. Without a server acting as an MTA, the claims merely recite the existence of a server for recording the dialog. But it is critical to the claims that the server function as the MTA—without this limitation, no structure is defined for conducting the message transmission. Consequently, the deletion of the preambles would create a structurally incomplete invention, which means they must be limiting. Furthermore, if the preambles were to be construed as non-limiting, the claims would necessarily be invalid over the prior art cited by the examiner during prosecution and admitted to by the applicant in the specification. *See, e.g.*,'913 patent 1:43-64 (acknowledging the existence of many e-mail systems and programs that provide for proof of delivery without the use of a server acting as a MTA).

2. Server Acting as a Mail Transport Agent

The BRI of "server acting as a Mail Transport Agent" is a server acting as a third party to relay a message from the sender to the intended recipient's Mail User Agent, and confirm delivery of the message. *See, e.g.*, '913 patent at 6:30-50; Fig. 1; 17:42-53; 23:55-24:5 and Fig. 6. This is the only interpretation supported by the specification. As mentioned above, the patentee distinguished the claimed invention over the prior art by stressing "the importance of storing the dialog [at the MTA server]. . . for later use in proof of the message and proof of the delivery of the message"). *See* Ex. 1003 at 1003.150-151.

According to the specification, storing the dialog on a third party server (i.e., neither the sender's server nor the recipient's server) ensures that the verification process is tamper proof. *See, e.g.*, '913 patent at 17:42-46 ("In sum, the system provides reliable evidence based on the testimony of a disinterested third party that a particular message having a particular content was sent, when it was sent, who sent it, who received it, when it was opened for reading, and when it was deleted."). Therefore, a server acting as a Mail Transport Agent must be construed as being a ***third-party server*** otherwise the verification process—the problem explicitly solved by the claimed invention according to the patentee—would not constitute "reliable proof of the content and delivery of electronic messages." *Id.* at 2:65-66.

VI. LEGAL STANDARD FOR PATENT VALIDITY

A. General Principles

A patent is invalid if it were granted in violation of one or more statutory or judicial requirements, including the requirements that: (1) the invention be novel, *i.e.*, not anticipated under 35 U.S.C. § 102; and (2) the invention not be unpatentable for obviousness under 35 U.S.C. § 103. Each of these requirements is discussed below.

B. Anticipation

To establish invalidity for lack of novelty, also referred to as "anticipation," 35 U.S.C. §102 has been interpreted to require that a single prior art reference disclose each and every element of the claimed invention, either expressly or inherently. *E.g.*, *Astra Aktiebolag v. Andrx Pharms.* (*In re Omeprazole Patent Litig.*), 483 F.3d 1364, 1371 (Fed. Cir. 2007); *Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d 1550, 1554 (Fed. Cir. 1995); *Minnesota Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992). In addition, to anticipate, a reference must enable one of ordinary skill in the art to make the anticipating subject matter. *Impax Labs., Inc. v. Aventis Pharms., Inc.*, 468 F.3d 1366, 1381 (Fed. Cir. 2006); *PPG Indus., Inc. v. Guardian Indus. Corp.*, 75 F.3d 1558, 1566 (Fed. Cir. 1996); *Akzo N.V. v. U.S. Int'l Trade Comm'n*, 808 F.2d 1471, 1479 (Fed. Cir. 1986), *cert. denied*, 482 U.S. 909 (1987).

Section 102(a) of the Patent Act bars entitlement to a patent when "the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent." 35 U.S.C. § 102(a) (2008).

C. Obviousness

Under the statutory provisions relating to obviousness, a patent may not be obtained "if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." 35 U.S.C. § 103(a) (2008). Obviousness determinations are made on a case-by-case basis after a factual inquiry has been made regarding the following considerations: (1) the scope and content of the prior art; (2) the differences between the prior art and the claimed invention; (3) the level of ordinary skill in the art; and (4) objective indicia of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727 (2007).

1. The Scope of the Pertinent Art

The courts rely on two criteria for determining whether a prior art reference is within the pertinent art and is therefore relevant in determining obviousness: (1) whether the reference is within the inventor's field of endeavor, regardless of

the problem being addressed; and (2) if the reference is not within the inventor's field of endeavor, whether the reference is reasonably pertinent to the problem with which the inventor was concerned, in which case the reference is considered to be in an analogous art. *E.g.*, *Princeton Biochemicals, Inc. v. Beckman Coulter, Inc.*, 411 F.3d 1332, 1339 (Fed. Cir. 2005); *Heidelberger Druckmaschinen AG v. Hantscho Commercial Prods., Inc.*, 21 F.3d 1068, 1071 (Fed. Cir. 1993); *In re Clay*, 966 F.2d 656, 658-59 (Fed. Cir. 1992). If either of these criteria are met, the reference is within the pertinent art and is relevant to the obviousness determination.

The appropriate field of endeavor is determined with reference to the explained subject matter of a patent application, including embodiments, function, and structure. *In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004). The claimed invention and the reference may be considered to be within the same field of endeavor if they have "essentially the same function and structure." *State Contracting & Eng'g Corp. v. Condotte Am., Inc.*, 346 F.3d 1057, 1069 (Fed. Cir. 2003); *In re Deminski*, 796 F.2d 436, 442 (Fed. Cir. 1986). A reference is reasonably pertinent to the problem with which the inventor was concerned if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of its subject matter, logically would have commended itself to the inventor's attention in considering his problem. *In re Icon Health & Fitness, Inc.*,

496 F.3d 1374, 1379-80 (Fed. Cir. 2007) (quoting *Clay*, 966 F.2d at 659); *accord In re GPAC*, 57 F.3d 1573, 1578 (Fed. Cir. 1995). Whether a reference logically would have been of interest to the inventor in considering his problem must be evaluated with reference to the time period in which the claimed invention was made, and not by importing the inventor's ultimate solution into the problem to be solved. *Monarch Knitting Mach. Corp. v. Sulzer Morat GmbH*, 139 F.3d 877, 881 (Fed. Cir. 1998).

2. The Level of Ordinary Skill in the Art

Obviousness is determined with reference to a hypothetical person of ordinary skill in the pertinent art —"not to . . . those skilled in remote arts, or to geniuses in the [pertinent] art." *Custom Accessories*, 807 F.2d at 962. The person of ordinary skill in the art is "one who thinks along the line of conventional wisdom in the art and is not one who undertakes to innovate." *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 454 (Fed. Cir. l985).

In *Environmental Designs, Ltd v. Union Oil Co. of California*, 713 F.2d 693, 696 (Fed. Cir. 1983), the Federal Circuit listed the factors that are considered in determining the level of ordinary skill in the art: (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers who are

active in the field. The hypothetical person of ordinary skill is presumed to be aware of all the pertinent art and the inventor's skill is not determinative. *Custom Accessories*, 807 F.2d at 962.

3. Obviousness Cannot Be Based on Hindsight Reconstruction of the Invention

There is no formula to show obviousness, rather one must show "a reason to combine the known elements in the fashion claimed by the patent at issue." *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007). Some rational underpinning must be provided to support such reasoning; conclusory statements are insufficient. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). A teaching, suggestion, or motivation for one ordinarily skilled in the art to combine elements at the time of the invention provides helpful insight into whether an invention is obvious, but should not be limited to information published in articles and patents. *KSR Int'l*, 127 S. Ct. at 1741. A reason for combining existing elements in an obvious manner may come from outside factors such as design and market demands, or common knowledge of those ordinarily skilled in the art. *Id*.

The teaching or suggestion to modify the prior art need not be expressly stated in the prior art. *B.F. Goodrich Co. v. Aircraft Braking Sys. Corp.*, 72 F.3d 1577, 1485 (Fed. Cir. 1996); *Cable Elec. Prods, Inc. v. Genmark Inc.*, 770 F.2d 1015, 1025 (Fed. Cir. 1985). The teaching or suggestion may be implicit in the prior art as the prior art would have been understood by one of ordinary skill. *See,*

e.g., *B.F. Goodrich*, 72 F.3d at 1485-83; *Cable Elec. Prods.*, 770 F.2d at 1025. It may also be found in the knowledge generally available to one of ordinary skill in the art. *See, e.g.*, *B.F. Goodrich*, 72 F.3d at 1583; *Cable Elec. Prods.*, 770 F.2d at 1025.

VII. DETAILED EXPLANATION OF GROUNDS FOR UNPATENTABILITY

The claim charts below provide a detailed explanation of the pertinence and manner of applying the prior art to claims 1-11 of the '913 patent. The portions cited herein are exemplary inasmuch as additional disclosure within these prior art documents teach the various elements of the claims of the '913 patent. The following is not intended to limit in any way the manner in which the disclosures in these references are applied to the '913 patent claims.

As discussed in detail above, during prosecution the applicant distinguished the inventions claimed in the '913 patent from the prior art using the "recording [and storing] at the server some portion of the selected one of the SMTP and ESMTP protocol dialog" limitation in independent claims 1 and 10. *See* Ex. 1003 at 1003.150. The dependent claims do not add any patentable subject matter.

For instance, claim 2 merely adds the step of "storing, the recorded dialog," and claim 3 merely adds the step of "returning to the sender an e-mail message including a copy of the recorded dialog." As admitted during the prosecution, both

of these limitations were well known prior to the filing of the ’913 patent and were not the reason behind allowing the ’913 patent. *Id.*

Dependent claim 4 further limits claim 1 by merely adding that the “e-mail message . . . has been digitally signed.” The ’913 patent specification admits that digital signature methods were known in the prior art. *See, e.g.*, ’913 patent at 3:55-63.

Dependent claim 5 further limits claim 1 by adding: “returning to the sender an e-mail message which includes: . . . an encrypted copy of dialog recorded by an encryption key that is not known by the sender of the message.” While dependent claim 6 further limits claim 1 by merely adding: “transmitting to the sender a message which includes: the recorded dialog, and an encrypted copy of a digital digest of the dialog recorded by an encryption key that is not known by the sender of the message.” Again, the ’913 patent specification admits that encryption methods were known in the prior art; therefore neither claim 5 nor claim 6 add any patentable subject matter. *See, e.g.*, ’913 patent at 7:36-52.

Dependent claim 7 further limits claim 1 by “computing a digital digest” and “saving the digital digest in some manner in which it may be associated with the message and the message sender and the recipient.” As discussed above, the ’913 patent specification admits that methods for computing a digital signature were known in the prior art. *See, e.g.*, ’913 patent at 3:55-63.

Dependent claim 8 further limits claim 7 by "returning to the sender an e-mail message which includes an encrypted copy of the original message, where the encryption key is not known by the sender of the message." As discussed above, the '913 patent specification admits that methods encrypting/decrypting data were known in the prior art. *See, e.g.*, '913 patent at 7:36-52.

Dependent claim 9 further limits claim 7 by adding: "returning to the sender an e-mail message which includes an encrypted copy of the digital digest of the original message where the encryption key is not known by the sender of the message. As discussed above, the '913 patent specification admits that methods for computing a digital signature and for encrypting/decrypting data were known in the prior art. *See, e.g.*, '913 patent at 3:55-63 and 7:36-52.

Dependent claim 11 further limits claim 10 by "decrypting" and "computing a digital digest" in order to authenticate the attachment. As discussed above, the '913 patent specification admits that methods for computing a digital signature and for encrypting/decrypting data were known in the prior art. *See, e.g.*, '913 patent at 3:55-63 and 7:36-52.

For at least this reasons, Petitioners submit that if independent claims 1 and 10 are found to be invalid, then the claims dependent on them must also be invalid.

A. Claims 1-11 are anticipated under 35 U.S.C. § 102 over Certified Exchange of Electronic Mail (CEEM)

CEEM teaches methods and systems for implementing a certified electronic mail exchange capable of assuring the receipt and integrity of the message. *See, e.g.*, Exhibit 1012. CEEM discloses using Message Transfer Agents (MTAs) as a trusted third party for transferring a message from the sender to the recipient. *See, e.g.*, Ex. 1012 at 1012.002. "The CEEM protocol employs a trusted third party to help solving the problem of physical exchange of the messages and to provide the proof of delivery from the recipient." Ex. 1012 at 1012.003; *see also, e.g.*, *id.* at Fig. 2.

"This protocol consists of four main elements: a trusted third party which is represented by the Email Office (EO), the originator, the recipient, and the communication medium. The EO is a third party server that provides the email handling service in an electronic manner." Ex. 1012 at 1012.003; *see also, e.g.*, *id.* at Fig. 2.

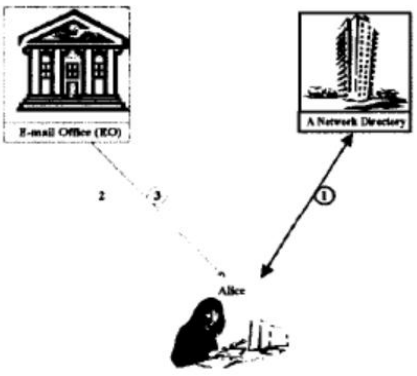


Figure 3. Message Preparation Phase.

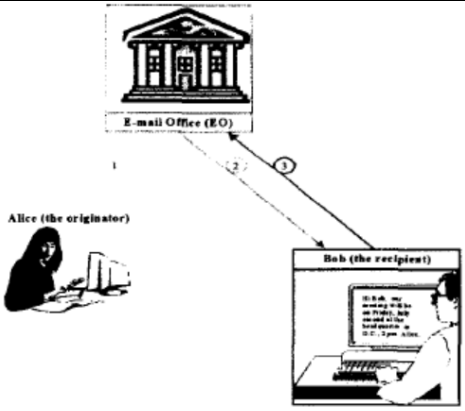


Figure 4. Message Delivery Phase.

For example, as shown above in Figs. 3-4, CEEM discloses that the sender ("Alice") hashes a message to produce a message digest, and then encrypts the message digest with her private key to produce a message signature. *Id*. at 43. The original message is concatenated with the message signature, and the concatenation is compressed and encrypted with a secret key generated by Alice. *Id.* After further processing of the message, Alice sends the message to the EO at step 1 of phase 2 of the protocol. *Id*. CEEM teaches that the EO receives the message from Alice and then decrypts the received message at step 2 of phase 2. *Id.* Figure 3 of the CEEM reference illustrates the message preparation phase of the CEEM protocol, and shows Alice transmitting a message to the EO (*i.e.*, the claimed server) at reference numeral 3. CEEM teaches that in phase 3 of the protocol, Bob accepts the message by signing a Certified Email Form ("CEF"), which is transmitted along with message. *Id.* Figure 4 of the CEEM reference illustrates the message

delivery phase of the CEEM protocol with the message being transmitted from the EO to recipient ("Bob") at reference numeral 2. *Id*.

Notably, CEEM explicitly mentions the existence of SMTP and teaches that the disclosed protocol is an extension of existing email protocols, such as SMTP. *Id*. at 1012.002, 1012.004. SMTP was first disclosed in RFC 821, dated 1982, which defines the dialog of the protocol including commands, replies, and so forth. *Id*. at 1012.002. Thus, one of ordinary skill in the art would have understood from CEEM that the EO in CEEM is configured to receive a mail transport protocol dialog (*i.e.*, SMTP dialog) when the message is transmitted from the EO to the recipient Bob. *See, e.g.,* Clark Decl. at ¶ 34.

CEEM also teaches using a database "to keep receipt of delivered email for certain time as stated in the Security Policies for future disputes. The basic principle of the CEEM is to simulate the real life post office certified mail with a practical solution to the problem of exchanging the email and the receipts at the delivery instance." Ex. 1012 at 1012.003; *see also, e.g., id.* at Fig. 2.

The following claim chart provides a detailed, but exemplary, explanation of the pertinence and manner of applying CEEM to claims 1-11 of the '913 patent.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
1. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This patent preamble is limiting because it is necessary to give life and meaning to the claim. Without the preamble and the recitation of the "Mail Transport Agent,"

	the alleged invention would be either inoperable or anticipated by the prior art that was cited during the prosecution. *See* Section V.C., *supra.* CEEM teaches that the "Simple Mail Transfer Protocol (SMTP) provides inter-machine email transfer services. It is the de facto protocol used by nearly all MTAs on the Internet. The UA communicates with the local MTA on behalf of the user to request message transfer. Then the local MTA communicates with a remote MTA on the destination system, or one on an intermediate relay, as shown in Figure 1." *See, e.g.*, Ex. 1012 at 1012.002; *see also, e.g., id*. at Fig. 1.
transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and	CEEM teaches that the "Simple Mail Transfer Protocol (SMTP) provides inter-machine email transfer services. It is the de facto protocol used by nearly all MTAs on the Internet. The UA communicates with the local MTA on behalf of the user to request message transfer. Then the local MTA communicates with a remote MTA on the destination system, or one on an intermediate relay, as shown in Figure1." *See, e.g.*, Ex. 1012 at 1012.002; *see also, e.g., id.* at Figs. 1 and 2 (describing a secure email delivery of messages based on the SMTP protocol).
recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message.	CEEM teaches using a database "to keep receipt of delivered email for certain time as stated in the Security Policies for future disputes. The basic principle of the CEEM is to simulate the real life post office certified mail with a practical solution to the problem of exchanging the email and the receipts at the delivery instance." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	**"Certified Exchange of Electronic Mail (CEEM)"**
2. The method as set forth in claim 1, including the step of: storing the recorded dialog in some form in which it may be associated with the message and the sender and the recipient of the message in such a way that it may be used to document the delivery history of the message from the sender to the recipient.	The CEEM Protocol section with respect to FIG. 2 notes that "[a]nother part of the database is used to keep receipt of delivered email for certain time as stated in the Security Policies for future disputes." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
3. The method as set forth in claim 1 including the step of: returning to the sender an e-mail message including a copy of the recorded dialog as proof of the successful delivery or failure to deliver the message to the recipient's mail server.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "form" to the sender and recipient as "a proof of delivery." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
4. The method as set forth in claim 1, including the step of: returning to the sender an e-mail message that has been digitally signed by an operator of the server and which includes the recorded dialog as evidence of the successful delivery or failure to deliver the message to the recipient's mail server.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery" Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
5. The method, as set forth in claim 1, including the step of: returning to the sender an e-mail message which includes: the recorded dialog, and an encrypted copy of	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery" and the "EO includes the

dialog recorded by an encryption key that is not known by the sender of the message.	message digest in the proof of delivery for any future dispute." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
6. The method as set forth in claim 1, including the step of: transmitting to the sender a message which includes: the recorded dialog, and an encrypted copy of a digital digest of the dialog recorded by an encryption key that is not known by the sender of the message.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery" and the "EO includes the message digest in the proof of delivery for any future dispute." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
7. The method as set forth in claim 1, further comprising: computing a digital digest of the message, and transmitting the message to the recipient, and saving the digital digest in some manner in which it may be associated with the message and the message sender and the recipient.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery" and the "EO includes the message digest in the proof of delivery for any future dispute." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
8. The method as set forth in claim 7, including the step of: returning to the sender an e-mail message which includes an encrypted copy of the original message, where the encryption key is not known by the sender of the message.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2. "Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest

	represents a unique 'fingerprint' of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4]. Then the message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to decrypt the message digest and he/she will recalculate the message digest of the received message. If both message digests (one generated by originator and the second generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered." Ex. 1012 at 1012.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
9. The method as set forth in claim 7, including the step of: returning to the sender an e-mail message which includes an encrypted copy of the digital digest of the original message where the encryption key is not known by the sender of the message.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed" "form" to the sender and recipient as "a proof of delivery" and the "EO includes the message digest in the proof of delivery for any future dispute." Ex. 1012 at 1012.003, *see also, e.g., id.* at Fig. 2. "Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest represents a unique 'fingerprint' of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4]. Then the

	message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to decrypt the message digest and he/she will recalculate the message digest of the received message. If both message digests (one generated by originator and the second generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered." Ex. 1012 at 1012.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
10. A method of transmitting a message and an attachment to the message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This patent preamble is limiting because it is necessary to give life and meaning to the claim. Without the preamble and the recitation of the "Mail Transport Agent," the alleged invention would be either inoperable or anticipated by the prior art that was cited during the prosecution. (*See above* Section V.C., *supra.* CEEM teaches that the "Simple Mail Transfer Protocol (SMTP) provides inter-machine email transfer services. It is the de facto protocol used by nearly all MTAs on the Internet. The UA communicates with the local MTA on behalf of the user to request message transfer. Then the local MTA communicates with a remote MTA on the destination system, or one on an intermediate relay, as shown in Figure 1." Ex. 1012 at 1012.002; *see also, e.g., id*. at Fig. 1.
transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and	CEEM teaches that the "Simple Mail Transfer Protocol (SMTP) provides inter-machine email transfer services. It is the de facto protocol used by nearly all MTAs on the Internet. The UA communicates with the

	local MTA on behalf of the user to request message transfer. Then the local MTA communicates with a remote MTA on the destination system, or one on an intermediate relay, as shown in Figure 1." Ex. 1012 at 1012.002, Fig. 1; *see also, e.g.*, *id.* at Figs. 1 and 2 (describing a secure email delivery of messages based on the SMTP protocol).
recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message;	CEEM teaches using a database "to keep receipt of delivered email for certain time as stated in the Security Policies for future disputes. The basic principle of the CEEM is to simulate the real life post office certified mail with a practical solution to the problem of exchanging the email and the receipts at the delivery instance." Ex. 1012 at 1012.003; *see also, e.g.*, *id.* at Fig. 2.
calculating a digital digest of the attachment,	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery." *See, e.g.*, Ex. 1012 at 1012.003; Fig. 2. "Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest represents a unique 'fingerprint' of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4]. Then the message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to

	decrypt the message digest and he/she will recalculate the message digest of the received message. If both message digests (one generated by originator and the second generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered." Ex. 1012 at 1012.
encrypting the digital digest of the attachment with an encryption key known only to a signer of the digital digest,	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery." *See, e.g.*, Ex. 1012 at 1012.003; *see also, e.g., id.* at Fig. 2. "Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest represents a unique 'fingerprint' of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4]. Then the message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to decrypt the message digest and he/she will recalculate the message digest of the received message. If both message digests (one generated by originator and the second generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered." *See, e.g.*, Ex. 1012 at 1012.
writing the encrypted digital digest of the attachment to a file which is attached to the message and,	CEEM teaches using a database "to keep receipt of delivered email for certain time as stated in the Security Policies for future

	disputes. The basic principle of the CEEM is to simulate the real life post office certified mail with a practical solution to the problem of exchanging the email and the receipts at the delivery instance." Ex. 1012 at 1012.003; *see also, e.g., id.* at Fig. 2.
transmitting the message and the file to a recipient.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery." *See, e.g.*, Ex. 1012 at 1012.003; *see also, e.g., id.* at Fig. 2.

US 8,224,913	"**Certified Exchange of Electronic Mail (CEEM)**"
11. In the method as set forth in claim 10, the step by the signer of: receiving a copy of the message and the file, decrypting the encrypted digital digest, computing a digital digest of the original attachment, and authenticating the attachment if and only if the values of the digital digests are equivalent.	The CEEM Protocol section with respect to FIG. 2 notes that the EO sends a "signed form" to the sender and recipient as "a proof of delivery." *See, e.g.*, Ex. 1012 at 1012.003; *see also, e.g., id.* at Fig. 2. "Digital signature guarantees the message integrity. To generate the digital signature, first a one way hash function transforms a variable-size input message and produces a fixed-size output string, which is called the message digest. The message digest represents a unique "fingerprint" of the message. Given the message digest it is impossible to guess the original message. In addition, there are no two messages that have the same message digests [4]. Then the message digest is encrypted using the private key of the originator and is appended to the message. The recipient will use the public key of the originator to decrypt the message digest and he/she will recalculate the message digest of the received message. If both message digests (one generated by originator and the second

	generated by recipient) are equal, then the integrity of the message is verified, otherwise the message has been altered." Ex. 1012 at 1012.

B. Claims 1-9 Are Anticipated under 35 U.S.C. § 102 over Certified Electronic Mail (CEM)

Certified Electronic Mail ("CEM") to Bahreman et al. is dated February 1994 and discloses in detail every element of every claim of the '913 patent. CEM teaches "protocols for certified electronic mail" using a "trusted third party" for enabling "two mutually suspicious users to exchange receipt for electronic mail." Ex. 1013 at 1013.003. The "CEM problem makes sense only in the presence of at least three parties—the sender, the recipient, and a third party." Ex. 1013 at 1013.005. "CEM is the digital equivalent of the post office providing certified mail (proof of mailing) and return receipt service for ordinary paper-based mail." Ex. 1013 at 1013.003.

CEM discloses a system including a sender (Sue), a recipient (Rob), and a trusted third party postmaster (PM). Ex. 1013 at 1013.006-007. The disclosed system enables a certified electronic mail to be transmitted from Sue to Rob through the PM. *Id*. at 1013.007. The PM provides proof of receipt of the message. *Id*. CEM states that the PM is a trusted third party and that the disclosed protocol can be implemented in modern communication networks on top of Privacy Enhanced Mail ("PEM"). *See id*. at 1013.003 ("CEM can also be implemented on

top of Privacy Enhanced Mail (PEM)"); *see also id.* at 1013.010 ("We have used a secure privatekey cryptosystem as a building block to our B-CEM protocol and have assumed a reliable communication channel using PEM.").

CEM states that sender Sue prepares and sends a CEM to the postmaster (*i.e.*, the server) in the first phase of the protocol. Ex. 1013 at 1013.006-008. CEM further instructs that "[e]very message exchanged among the parties in the protocol consists of a content section (or body) and a header section" to "allow Multipurpose Internet Mail Extension (MIME) capable mail user agents to be used to interface with users." *Id*. at 1013.007. One of ordinary skill in the art would have understood that such User Agents are used to compose "a message." Further, CEM discloses that in the second phase of the protocol the postmaster (*i.e.*, the server) generates a pseudorandom number, enciphers the CEM, signs the resultant ciphertext, and transmits the signed ciphertext to recipient Rob. *Id*. at 1013.008. Figure 1, which is reproduced below, provides a high-level overview of the B-CEM protocol and illustrates sender Sue transmitting a CEM to the PM (*i.e.*, the server), which then transmits the ciphertext of the CEM to recipient Rob.

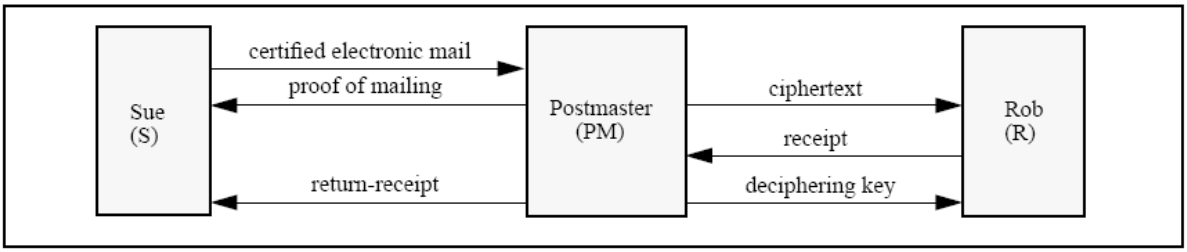


Figure 1. High-level overview of the interactions among the parties in a B-CEM protocol.

Figures 1 and 7 illustrate that Rob transmits the receipt, which provides an indication of receipt of the message stored within the ciphertext, to the PM. *Id*. at 1013.006 and 1013.008. CEM teaches that the transmission of messages between the parties can take the form of MIME messages and that CEM can be implemented at the application layer of the ISO OSI Reference Model on top of PEM. *Id*. at 1013.003. One of ordinary skill in the art would understand that PEM describes a message transfer system that includes a number of mail transfer agents ("MTAs") for relaying messages and delivering them to intended recipients ("UAs") used for reading and composing messages. Clark Decl. at ¶¶ 35-36. The transmission of messages between the MTAs and UAs utilize protocol handshakes or dialogs (*i.e.*, SMTP or POP). Clark Decl. at ¶ 34.

Consequently, one of ordinary skill in the art would have understood from the foregoing teachings that the PM is capable of being configured by editing an MTA config file to receive and store a mail transport protocol dialog during the transmission of the ciphertext (message) to recipient Rob. Clark Decl. at ¶ 35.

CEM also teaches that:

> CEM users could enjoy confidentiality, authenticity, integrity, and non-repudiation of message origin in addition to proof of mailing and non-repudiation of message receipt. Briefly, confidentiality protects transmitted messages from unauthorized disclosure. Integrity ensures that the message content is not modified during transmission.

> Authentication is simply the assurance that the remote entity sending the message is correctly identified. Non-repudiation comes in two flavors, non-repudiation of message origin and non-repudiation of message receipt. The former protects against the sender denying transmission of the message while the latter protects against the recipient denying receipt of the message. Proof of mailing allows the sender to prove to any third party that the sender did in fact send the message to the recipient.

Ex. 1013 at 1013.003.

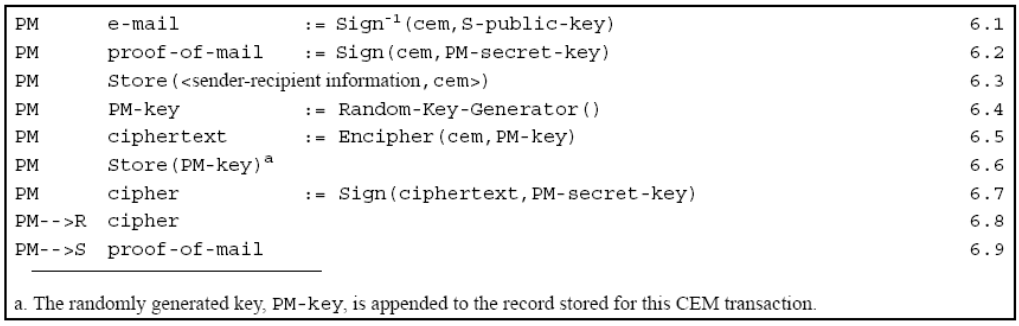
What is taught by CEM is exactly what is claimed by the ’913 patent. The specification of the ’913 patent identified the problem solved as exactly the problem being solved by CEM. The ’913 patent states:

> There exists a need for an e-mail system and/or method that can provide reliable proof of the content and delivery of an e-mail message in order to take fuller advantage of the convenience and low cost of communicating via e-mail.

’913 patent 2:17-20.

CEM discloses that the PM checks the validity of the receipt and appends the receipt to the stored record, which includes sender-recipient information, the CEM, and the randomly generated key in the fourth phase of the protocol. Ex. 1013 at 1013.008-009. Additionally, CEM states that the PM signs and sends two messages in phase four with one of them being a return-receipt to sender Sue, which includes the receipt or the indication of receipt. Figure 6, which is

reproduced below, illustrates that the sender-recipient information (e.g., at least a portion of the mail transport protocol dialog) is part of the stored record at 6.2.



```
PM      e-mail          := Sign-1(cem,S-public-key)                    6.1
PM      proof-of-mail   := Sign(cem,PM-secret-key)                     6.2
PM      Store(<sender-recipient information,cem>)                      6.3
PM      PM-key          := Random-Key-Generator()                      6.4
PM      ciphertext      := Encipher(cem,PM-key)                        6.5
PM      Store(PM-key)[a]                                               6.6
PM      cipher          := Sign(ciphertext,PM-secret-key)              6.7
PM-->R  cipher                                                         6.8
PM-->S  proof-of-mail                                                  6.9
```

a. The randomly generated key, PM-key, is appended to the record stored for this CEM transaction.

Figure 6. Phase two of a B-CEM protocol. Postmaster receives cem and forwards to recipient.

Ex. 1013 at 1013.008.

Consequently, as shown below in further detail, CEM solves the problem stated by the ’913 specification in the same manner recited in the ’913 claims more than five years prior to the earliest priority date of the ’913 patent.

US 8,224,913	“**Certified Electronic Mail**” **(CEM)**
1. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This patent preamble is limiting because it is necessary to give life and meaning to the claim. In fact, without the preamble and the recitation of the “Mail Transport Agent,” the alleged invention would be either inoperable or anticipated by the prior art that was cited during the prosecution. *See, e.g.*, Exhibit 1013 at Fig. 1 (*See* section V.C., *supra.* where sender “Sue(S)” transmits a “certified electronic mail” to a “**Postmaster (PM),**” acting as the claimed MTA by transmitting the ciphertext to recipient “Rob(R)”); *see also, e.g.*, *id.* at 4; Fig.1.
transmitting the message to the recipient's	*See, e.g.*, FIG. 1 (where sender “Sue(S)”

Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and	transmits a "certified electronic mail" to a "Postmaster (PM)", which in turn transmits the ciphertext to recipient "Rob(R)"); *see, e.g.*, Ex. 1013 at 1013.006; Fig.1.
recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message.	CEM discloses that the PM checks the validity of the receipt and appends the receipt to the stored record, which includes sender-recipient information, the CEM, and the randomly generated key in the fourth phase of the protocol. Additionally, CEM states that the PM signs and sends two messages in phase four with one of them being a return-receipt to sender Sue, which includes the receipt or the indication of receipt. *See, e.g.*, Ex. 1013 at 1013.008-009; Figs. 6 and 8. See also discussion in section titled "Phase Four" and FIG. 8 which explicitly mention that the postmaster stores a "receipt" in a "stored record" as "this is useful for future inquiries" "should a dispute occur between the parties" and "the record maintained by the postmaster can be presented to a judge." *Id.* Also, see section VII titled "Stable Storage with Strict Access Control Mechanism" which further states that the storage is used "for maintaining records of CEM transactions." Ex. 1013 at 1013.009.

US 8,224,913	"**Certified Electronic Mail**"
2. The method as set forth in claim 1, including the step of: storing the recorded dialog in some form in which it may be associated with the message and the sender and the recipient of the message in such a	See description of "Phase two" which states that the postmaster stores, in its memory, a "record" that includes sender-recipient information, a timestamp, and the message where this "record can serve as proof of

way that it may be used to document the delivery history of the message from the sender to the recipient.	mailing" of sender. *See, e.g.*, Ex. 1013 at 1013.008-009; Figs. 6 and 8. Also, see description of "Phase four" which states that the "receipt" that is obtained from the recipient is added to the "stored record" wherein "should a dispute occur between the parties, the record maintained by the postmaster can be presented to a judge." *Id.*

US 8,224,913	"**Certified Electronic Mail**"
3. The method as set forth in claim 1 including the step of: returning to the sender an e-mail message including a copy of the recorded dialog as proof of the successful delivery or failure to deliver the message to the recipient's mail server.	See description of "Phase two" and "Phase four" which indicate that the sender is sent a "proof of mailing" once a mail is received at the postmaster and a "receipt" once the mail was delivered to the recipient. *See, e.g.*, Ex. 1013 at 1013.008-009; Figs. 6 and 8.

US 8,224,913	"**Certified Electronic Mail**"
4. The method as set forth in claim 1, including the step of: returning to the sender an e-mail message that has been digitally signed by an operator of the server and which includes the recorded dialog as evidence of the successful delivery or failure to deliver the message to the recipient's mail server.	In the description of "Phase two", it is noted that "the postmaster can sign" the sender's certified electronic message (CEM) and "return it" to the sender as proof of mailing *See, e.g.*, Ex. 1013 at 1013.008, Fig. 6, step 6.2 "proof-of-mail."

US 8,224,913	"**Certified Electronic Mail**"
5. The method, as set forth in claim 1, including the step of: returning to the sender an e-mail message which includes: the recorded dialog, and an encrypted copy of dialog recorded by an encryption key that is not known by the sender of the message.	In the description of "Phase two", it is noted that "the postmaster can sign" the sender's certified electronic message (CEM) and "return it" to the sender as proof of mailing (see FIG. 6, step 6.2 "proof-of-mail") wherein the "proof-of-mail" is based on signing using a "PM-secret-key" which does not appear to be known to a sender. *See, e.g.*, Ex. 1013 at 1013.008, Fig. 6, step 6.2 "proof-of-mail."

US 8,224,913	"**Certified Electronic Mail**"
6. The method as set forth in claim 1, including the step of: transmitting to the sender a message which includes: the recorded dialog, and an encrypted copy of a digital digest of the dialog recorded by an encryption key that is not known by the sender of the message.	In the description of "Phase two", it is noted that "the postmaster can sign" the sender's certified electronic message (CEM) and "return it" to the sender as proof of mailing (see FIG. 6, step 6.2 "proof-of-mail") wherein the "proof-of-mail" is based on signing using a "PM-secret-key" which does not appear to be known to a sender. *See, e.g.*, Ex. 1013 at 1013.008, Fig. 6, step 6.2 "proof-of-mail." In the "Notation" section it is noted that "a message digest or hash value of the email is signed instead of the email itself" and in the "implementing the postmaster" section, the authors state that "storage requirements can be reduced by storing the message digest instead of the message itself" where "message digests may be obtained by applying a one-way hash function…to the message" where the "hash can then be used to facilitate retrieval of records pertaining to a particular CEM transaction." *See, e.g.*, Ex. 1013 at 1013.006.

US 8,224,913	"**Certified Electronic Mail**"
7. The method as set forth in claim 1, further comprising: computing a digital digest of the message, and transmitting the message to the recipient, and saving the digital digest in some manner in which it may be associated with the message and the message sender and the recipient.	In the "Notation" section it is noted that "a message digest or hash value of the email is signed instead of the email itself" and in the "implementing the postmaster" section, the authors state that "storage requirements can be reduced by storing the message digest instead of the message itself" where "message digests may be obtained by applying a one-way hash function…to the message" where the "hash can then be used to facilitate retrieval of records pertaining to a particular CEM transaction." Ex. 1013 at

	1013.006.

US 8,224,913	"**Certified Electronic Mail**"
8. The method as set forth in claim 7, including the step of: returning to the sender an e-mail message which includes an encrypted copy of the original message, where the encryption key is not known by the sender of the message.	In the description of "Phase two", it is noted that "the postmaster can sign" the sender's certified electronic message (CEM) and "return it" to the sender as proof of mailing (see Fig. 6, step 6.2 "proof-of-mail") wherein the "proof-of-mail" is based on signing using a "PM-secret-key" which does not appear to be known to a sender. *See, e.g.*, Ex. 1013 at 1013.008, Fig. 6, step 6.2 "proof-of-mail."

US 8,224,913	"**Certified Electronic Mail**"
9. The method as set forth in claim 7, including the step of: returning to the sender an e-mail message which includes an encrypted copy of the digital digest of the original message where the encryption key is not known by the sender of the message.	In the description of "Phase two", it is noted that "the postmaster can sign" the sender's certified electronic message (CEM) and "return it" to the sender as proof of mailing (see Fig. 6, step 6.2 "proof-of-mail") wherein the "proof-of-mail" is based on signing using a "PM-secret-key" which does not appear to be known to a sender. *See, e.g.*, Ex. 1013 at 1013.008, Fig. 6, step 6.2 "proof-of-mail." In the "Notation" section it is noted that "a message digest or hash value of the email is signed instead of the email itself" and in the "implementing the postmaster" section, the authors state that "storage requirements can be reduced by storing the message digest instead of the message itself" where "message digests may be obtained by applying a one-way hash function . . . to the message" where the "hash can then be used to facilitate retrieval of records pertaining to a particular CEM transaction." Ex. 1013 at 1013.006-007.

For at least the above mentioned reasons, claim 1-9 of the ’913 patent is anticipated by CEM.

C. Claims 10-11 are rendered obvious under 35 U.S.C. § 103 over CEM in view of Privacy Enhanced Mail (“PEM”)

As discussed above, CEM instructs that it can be combined with other e-mail utilities such as Privacy Enhanced Mail (“PEM”). *See, e.g.*, CEM at 1, 2, 5, 8 and 16 (“CEM can also be implemented on top of Privacy Enhanced Mail (PEM).” Consequently, there exists not only a motivation to combine CEM and PEM, but a clear instruction to do so.

“PEM is an Internet standard that provides for secure exchange of electronic mail. PEM employs a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity. The message integrity aspects allow the user to ensure that a message hasn’t been modified during transport from the sender. The sender authentication allows a user to verify that the PEM message that they have received is truly from the person who claims to have sent it. The confidentiality feature allows a message to be kept secret from people to whom the message was not addressed.” Exhibit 1014, *available at* http://www.csee.umbc.edu/~woodcock/cmsc482/proj1/pem.html. PEM was “used with just about any program capable of generating Internet mail.” *Id.*

US 8,224,913	"Certified Electronic Mail" in view of Privacy Enhanced Mail ("PEM")
10. A method of transmitting a message and an attachment to the message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This patent preamble is limiting because it is necessary to give life and meaning to the claim. In fact, without the preamble and the recitation of the "Mail Transport Agent," the alleged invention would be either inoperable or anticipated by the prior art that was cited during the prosecution. *See* section V.C., *supra.*
transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and	*See, e.g.*, Exhibit 1013 Fig. 1, where sender "Sue(S)" transmits a "certified electronic mail" to a "Postmaster (PM)", which in turn transmits the ciphertext to recipient "Rob(R)."
recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message;	CEM discloses that the PM checks the validity of the receipt and appends the receipt to the stored record, which includes sender-recipient information, the CEM, and the randomly generated key in the fourth phase of the protocol. Additionally, CEM states that the PM signs and sends two messages in phase four with one of them being a return-receipt to sender Sue, which includes the receipt or the indication of receipt. *See, e.g.*, Ex. 1013 at 1013.008; Figs. 6 and 8. See also discussion in section titled "Phase Four" and FIG. 8 which explicitly mention that the postmaster stores a "receipt" in a "stored record" as "this is useful for future inquiries" "should a dispute occur between the parties" and "the record maintained by the postmaster can be presented to a judge." *Id.*

	Also, see section VII titled "Stable Storage with Strict Access Control Mechanism" which further states that the storage is used "for maintaining records of CEM transactions." *Id.* at 1013.009.
calculating a digital digest of the attachment, encrypting the digital digest of the attachment with an encryption key known only to a signer of the digital digest, writing the encrypted digital digest of the attachment to a file which is attached to the message and, transmitting the message and the file to a recipient.	PEM discloses the "concept known as a message digest." In PEM, messages are given a 16-octet value, which "is then encrypted with whichever key management technique is currently in use." Ex. 1014 at 1014.003. "When the message is received, the recipient can also run the message digest on the message, and if it hasn't been modified in-transit, the recipient can be reasonably assured that the message hasn't been tampered with maliciously." *Id.* "Data Encrypting Keys (DEKs) are used for encryption of message text and (with certain choices among a set of alternative algorithms) for computation of message integrity check (MIC) quantities. In the asymmetric key management environment, DEKs are also used to encrypt the signed representations of MICs in PEM messages to which confidentiality has been applied." RFC 1421 *available at* http://tools.ietf.org/html/rfc1421, attached as Exhibit 1015. "When PEM processing is to be performed on an outgoing message, a DEK is generated for use in message encryption." *Id.*

US 8,224,913	"Certified Electronic Mail" in view of Privacy Enhanced Mail ("PEM")
11. In the method as set forth in claim 10, the step by the signer of: receiving a copy of the message and the file, decrypting the encrypted digital digest, computing a digital digest of the original attachment, and authenticating the attachment if and only if the values of the digital digests are equivalent.	PEM discloses the "concept known as a message digest." In PEM, messages are given a 16-octet value, which "is then encrypted with whichever key management technique is currently in use." Ex. 1014 at 1014.003. "When the message is received, the recipient can also run the message digest on the message, and if it hasn't been modified in-transit, the recipient can be reasonably assured that the message hasn't been tampered with maliciously." *Id*. When a PEM message is received, the cryptographic control fields within its encapsulated header provide the information required for each authorized recipient to perform MIC validation and decryption of the received message text. For ENCRYPTED and MIC-ONLY messages, the printable encoding is converted to a bitstring. Encrypted portions of the transmitted message are decrypted. The MIC is validated. Then, the recipient PEM process converts the canonical representation to its appropriate local form." RFC 1421 *available at* http://tools.ietf.org/html/rfc1421, attached as Exhibit 1015.

D. Claims 1-3 are anticipated under 35 U.S.C. § 102 over Postfix

Postfix is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail. intended as an alternative to the widely used Sendmail

MTA. Postfix was originally written in 1997 and was widely released in December 1998 as "Secure Mailer." *See, e.g.*, Sharing Software, IBM to Release Mail Program Blueprint, Dec. 14, 1998, *available at* http://www.nytimes.com/library/tech/98/12/biztech/articles/14blue.html; *see also, e.g.*, Venema Aims to Make Network Software Safe, Oct. 2, 1998, *available at* http://www.postfix.org/developer.199810.html.

Postfix has been one of the more popular MTA's since the late 1990's. Clark Decl. at ¶ 36. The release notes from the 1999 version of Postfix show that it contained access protocol commands for junk mail handling, e-mail delivery delays, and bounced messages since at least January 1999. *See* Postfix Release Notes, http://web.archive.org/web/19990508202510/http:/www.postfix.org/RELEASE_ NOTES, attached as Exhibit 1016,

As shown below in detail, Postfix anticipates claims 1-3 of the '913 patent prior to its earliest priority date.

US 8,224,913	**Postfix**
1. A method of transmitting a message from a sender to a recipient through a server acting as a Mail Transport Agent, including the steps at the server of:	This patent preamble is limiting because it is necessary to give life and meaning to the claim. In fact, without the preamble and the recitation of the "Mail Transport Agent," the alleged invention would be either inoperable or anticipated by the prior art that was cited during the prosecution. *See* section V.C., *supra*. Postfix is a free open-source mail transfer agent (MTA) that routes and delivers e-mail. Postfix was originally written in 1997 and was widely released in December 1998 as "Secure Mailer." *See, e.g.*, John Markoff, *Sharing Software, IBM to*

	Release Mail Program Blueprint (Dec. 14, 1998), http://www.nytimes.com/library/tech/98/12/biztech/articles/14blue.html, attached as Ex. 1017; *see also, e.g.*, Cameron Laird, *Venema Aims to Make Network Software Safe* (Oct. 2, 1998), http://www.postfix.org/developer.199810.html, attached as Exhibit 1018
transmitting the message to the recipient's Mail Transport Agent in a protocol dialog selected from a group consisting of the selected one of the SMTP and ESMTP protocols; and	Postfix transmits e-mail using SMTP. *See, e.g.*, December 11, 1999 Postfix source code at smtp.8, attached as Exhibit 1019: ("The SMTP client processes message delivery requests from the queue manager. Each request specifies a queue file, a sender address, a domain or host to deliver to, and recipient information. . . . The SMTP client updates the queue file and marks recipients as finished, or it informs the queue manager that delivery should be tried again at a later time. . . . The SMTP client looks up a list of mail exchanger addresses for the destination host, sorts the list by preference, and connects to each listed address until it finds a server that responds.").
recording at the server some portion of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient through the server including those portions of the selected one of the SMTP and ESMTP protocol dialog between the server and the recipient in which the receiving Mail Transport Agent accepts or declines delivery of the transmitted message.	Postfix records, at the server, part of the dialog showing whether the MTA accepts or declines the e-mail transmission. *See, e.g.*, December 11, 1999 Postfix source code at smtp.8, attached as Exhibit 1019: ("The SMTP client updates the queue file and marks recipients as finished, or it informs the queue manager that delivery should be tried again at a later time. Delivery problem reports are sent to the **bounce(8)** or **defer(8)** daemon as appropriate. . . . Depending on the setting of the **notify_classes** parameter, the postmaster is notified of bounces, protocol problems, and of other trouble."); *see also, e.g.*, *id.* at sendmail.c, attached as Exhibit 1020 ("Specific command aliases are provided for other common modes of operation: **mailq** List the mail queue. Each entry shows the queue file ID, message size, arrival time, sender, and the recipients that still need to be delivered. If mail could not be delivered upon the last attempt, the reason for failure is shown. This mode of operation is implemented by connecting to the **showq(8)** daemon.").

US 8,224,913	Postfix
2. The method as set forth in claim 1, including the step of: storing the recorded dialog in some form in which it may be associated with the message and the sender and the recipient of the message in such a way that it may be used to document the delivery history of the message from the sender to the recipient.	Postfix stores dialog in a way that it may be used to document the delivery history of the message form the sender to the recipient. *See, e.g.*, Exhibit 1019 December 11, 1999 Postfix source code at smtp.8: ("The SMTP client updates the queue file and marks recipients as finished, or it informs the queue manager that delivery should be tried again at a later time. Delivery problem reports are sent to the **bounce(8)** or **defer(8)** daemon as appropriate. . . . Depending on the setting of the **notify_classes** parameter, the postmaster is notified of bounces, protocol problems, and of other trouble."); *see also, e.g.*, *id.* at bounce.8 attached as Exhibit 1021 ("The **bounce** daemon maintains per-message log files with non-delivery status information. Each log file is named after the queue file that it corresponds to, and is kept in a queue subdirectory named after the service name in the **master.cf** file (either **bounce** or **defer**). . . . The **bounce** daemon processes two types of service requests: • Append a recipient status record to a per-message log file. • Post a bounce message, with a copy of a log file and of the corresponding message. When the bounce is posted successfully, the log file is deleted. The software does a best effort to notify the sender that there was a problem. A notification is sent even when the log file or original message cannot be read.").

US 8,224,913	Postfix
3. The method as set forth in claim 1 including the step of: returning to the sender an e-mail message including a copy of the recorded dialog as proof of the successful delivery or failure to deliver the message to the recipient's mail server.	Postfix returns to the sender an e-mail message including a copy of the log file as proof of failure to deliver the message. *See, e.g.*, Exhibit 1021, December 11, 1999 Postfix source code at bounce.8 ("The **bounce** daemon maintains per-message log files with non-delivery status information. Each log file is named after the queue file that it corresponds to, and is kept in a queue subdirectory named after the service name in the **master.cf** file (either **bounce** or **defer**). . . . The **bounce** daemon processes two types of service requests: • Append a recipient status record to a per-message log file. • Post a bounce message, with a copy of a log file and of the corresponding message. When the bounce is posted successfully, the log file is deleted. The software does a best effort to notify the sender that there was a problem. A notification is sent even when the log file or original message cannot be read."); *see also, e.g., id.* at RELEASE_NOTES ("Automatic notification of delayed mail (disabled by default). With delay_warning_time = 4", Postfix informs senders when mail has not been delivered after 4 hours.") *id.* at error.c, attached as Exhibit 1022 ("The error mailer client forces all recipients to bounce, using the domain or host information as the reason for non-delivery, updates the queue file and marks recipients as finished, or it informs the queue manager that delivery should be tried again at a later time.")

VIII. CONCLUSION

For the foregoing reasons, claims 1-11 (all claims) of the ’913 patent are unpatentable. Petitioners therefore request that a post-grant review of these claims be instituted pursuant to 35 U.S.C. § 324. Petitioners reserve the right to apply additional prior art and arguments, depending on what arguments or amendments Patent Owner might present. Petitioners also reserve the right to cite and apply any additional art that it might discover as relevant to the issued claims or any amended claims, as the post-grant review proceeds.

IX. FEE STATEMENT (37 C.F.R. §42.15(B))

Petitioners include the payment of a fee of $12,000. If there are any additional fees due in connection with the filing of this paper, please charge the required fees to our deposit account no. 50-2036.

Respectfully submitted,

Dated: October 11, 2013

By: /Ken Sheehan/
Kenneth J. Sheehan, Lead Counsel
Registration No. 36,270
Shawnna M. Yashar, Backup Counsel
Registration No. 59,624
BAKER & HOSTETLER LLP
1050 Connecticut Ave. NW
Washington Square, Ste. 1100
Washington, DC 20036
Tel: (202) 861-1500
Fax: (202) 861-1783
ksheehan@bakerlaw.com
syashar@bakerlaw.com

ATTORNEYS FOR PETITIONER
EXPERIAN MARKETING SOLUTIONS, INC.

By:/ArthurDresner/
Arthur Dresner, Lead Counsel
Registration No. 24,403
Jordana Garellek, Backup Counsel
Registration No. 67,859
Duane Morris LLP
1540 Broadway
New York, NY 10036-4086
Telephone: (212) 692-1014
Facsimile: (212) 202-4904
ADresner@duanemorris.com
JGarellek@duanemorris.com

Jarrad M. Gunther, Reg. No. 63,903
Back-up Counsel
Duane Morris LLP
30 S. 17th Street
Philadelphia, PA 19103
Telephone: (215) 979-1000
Facsimile: (215) 979-1020
JMGunther@duanemorris.com

ATTORNEYS FOR PETITIONER
EPSILON DATA MANAGEMENT, LLC

EXHIBIT LIST	
Exhibit 1001	U.S. Patent No. 8,224,913 – System and Method for Verifying Delivery and Integrity of Electronic Messages.
Exhibit 1002	Recorded Assignments for U.S. Patent No. 8,224,913.
Exhibit 1003	Prosecution File History of U.S. Patent No. 8,224,913.
Exhibit 1004	Encyclopedia Britannica, "E-Commerce" *available at:* http://www.britannica.com/EBchecked/topic/183748/e-commerce.
Exhibit 1005	Registered Email for Financial Services, RPost (Oct. 9, 2013) *available at:* http://www.rpost.com/industries/financial-services.
Exhibit 1006	RPost Product Manager, *Bank uses eSignOff services for international clients*, RPost Blog (Dec. 13, 2010), *available at:* http://www.rpost.com/blog/548-bank-uses-esignoff-services-for-international-clients.
Exhibit 1007	ePostal News Press Release, *ePostal Goodmail lawsuit* (Oct. 5, 2009), *available at:* http://www.rpost.com/news-and-events/press-room/media-coverage/341.
Exhibit 1008	RPost Product Manager, *RPost's electronic signature services used to record signoff on international sales contracts*, RPost Blog (Dec. 9, 2010), *available at:* http://www.rpost.com/blog/543-rposts-electronic-signature-services-used-to-record-signoff-on-international-sales-contracts.
Exhibit 1009	RPost's First Amended Complaint Against Epsilon dated September 13, 2013, in *RPost Holdings, Inc. v. Epsilon Data Management, LLC*, E.D. Tex. No. 2:12-cv-00511-JRG.
Exhibit 1010	RPost's First Amended Complaint Against Experian dated August 30, 2013, in *RPost Holdings, Inc. v. Experian Marketing Solutions, Inc.*, E.D. Tex. No. 2:12-cv-00513-JRG (consolidated with -00511).
Exhibit 1011	PURPOSEFULLY OMITTED
Exhibit 1012	B. Al-Hammadi et al., *Certified Exchange of Electronic Mail (CEEM)*, Proceedings IEEE Southeastcon '99, March 25 – 28, 1999.
Exhibit 1013	A. Bahreman et al., *Certified Electronic Mail (CEM)*, In Proceedings of the 1994 Network and Distributed Systems Security Conference, February 1994.

Exhibit 1014	Michael A. Gurski, *Privacy-Enhanced Mail ("PEM")*, Oct. 24, 1995, *available at:* http://www.csee.umbc.edu/~woodcock/cmsc482/proj1/pem.html.
Exhibit 1015	J. Linn, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*, Network Working Group Request for Comments 1421 (February 1993), http://tools.ietf.org/html/rfc1421.
Exhibit 1016	Release notes from the 1999 version of Postfix, *available at:* http://web.archive.org/web/19990508202510/http:/www.postfix.org/RELEASE_NOTES.
Exhibit 1017	John Markoff, *Sharing Software, IBM to Release Mail Program Blueprint* (Dec. 14, 1998), *available at:* http://www.nytimes.com/library/tech/98/12/biztech/articles/14blue.html.
Exhibit 1018	Cameron Laird, *Venema Aims to Make Network Software Safe* (Oct. 2, 1998), *available at:* http://www.postfix.org/developer.199810.html.
Exhibit 1019	Postfix source code, December 11, 1999 version *available at:* ftp://mirrors.loonybin.net/pub/postfix/index.html at smtp.8
Exhibit 1020	Postfix source code, December 11, 1999 version *available at:* ftp://mirrors.loonybin.net/pub/postfix/index.html at sendmail.c.
Exhibit 1021	Postfix source code, December 11, 1999 version *available at:* ftp://mirrors.loonybin.net/pub/postfix/index.html at bounce.8.
Exhibit 1022	Postfix source code, December 11, 1999 version *available at:* ftp://mirrors.loonybin.net/pub/postfix/index.html at error.c.
Exhibit 1023	Declaration of Paul C. Clark, DSc. with Appendix 1.

CERTIFICATE OF SERVICE (37 C.F.R. §§ 42.6(e), 42.105(a))

The undersigned certifies that on October 11, 2013, a complete and entire copy of this Petition for Covered Business Method Patent Review and all supporting exhibits were provided via Express Mail, costs prepaid, to the Patent Owner by serving the correspondence address of record as follows:

Winston O. Huff, Attorney in Charge
State Bar No. 24068745
Deborah Jagai
State Bar No. 24048571
W. O. Huff & Associates, PLLC
302 Market Street, Suite 450
Dallas, Texas 75202
214.749.1220 (Firm)
469.206.2173 (Facsimile)
whuff@huffip.com
djagai@huffip.com

Lewis E. Hudnell, III
Colvin Hudnell LLP
375 Park Avenue
Suite 2607
New York, New York 10152
Tel: 212.634.6844
Fax: 347.772.3034
lewis@colvinhudnell.com

/Shawnna Yashar/ (Reg. # 59,624)

Shawnna M. Yashar
BAKER & HOSTETLER LLP
1050 Connecticut Ave. NW
Washington Square, Ste. 1100
Washington, DC 20036
Tel: (202) 861-1500
Fax: (202) 861-1783
syashar@bakerlaw.com