BRETT J. WILLIAMSON (S.B. 145235)
bwilliamson@omm.com
O'MELVENY & MYERS LLP
610 Newport Center Drive, 17th Floor
Newport Beach, California 92660-6429
Telephone: (949) 760-9600
Facsimile: (949) 823-6994

RYAN K. YAGURA (S.B. 197619)
ryagura@omm.com
VISION L. WINTER (S.B. 234172)
vwinter@omm.com
O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000
Facsimile: (213) 430-6407

Attorneys for Plaintiff Secured Mail Solutions, LLC

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

SECURED MAIL SOLUTIONS, LLC,

Plaintiff,

v.

HARTE-HANKS, INC., HARTE-HANKS DIRECT, INC., HARTE-HANKS DIRECT MARKETING/BALTIMORE, INC., HARTE-HANKS DIRECT MARKETING/CINCINNATI, INC., HARTE-HANKS DIRECT MARKETING /DALLAS, INC., HARTE-HANKS DIRECT MARKETING/FULLERTON, INC., HARTE-HANKS DIRECT MARKETING/JACKSONVILLE, LLC, HARTE-HANKS DIRECT MARKETING/KANSAS CITY, LLC, and HARTE-HANKS PRINT, INC.

Defendant.

Case No. SA-CV-12-01118 DOC

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

JURY DEMAND

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Secured Mail Solutions, LLC files this first amended complaint for patent infringement against Defendants Harte-Hanks, Inc., Harte-Hanks Direct, Inc., Harte-Hanks Direct Marketing/Baltimore, Inc., Harte-Hanks Direct Marketing/Cincinnati, Inc., Harte-Hanks Direct Marketing/Dallas, Inc., Harte-Hanks Direct Marketing/Fullerton Inc., Harte-Hanks Direct Marketing/Jacksonville, LLC, Harte-Hanks Direct Marketing./Kansas City, LLC, and Harte-Hanks Print, Inc. Plaintiff Secured Mail Solutions LLC alleges:

THE PARTIES

1. Secured Mail Solutions, LLC ("SMS") is a limited liability company duly organized under the laws of the state of Nevada, with its principal place of business at 9550 S. Eastern Ave., Suite 253, Las Vegas, NV 89123.

2. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks, Inc. is a corporation duly organized and existing under the laws of the state of Delaware, with its principal place of business at 9601 Mcallister Freeway, Suite 610 San Antonio, TX 78216.

3. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct, Inc. is a corporation duly organized and existing under the laws of the state of New York, with its principal place of business at 9601 Mcallister Freeway, Suite 610, San Antonio, TX 78216.

4. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Baltimore, Inc. is a corporation duly organized and existing under the laws of the state of Maryland, with its principal place of business at 1414 Russell Street, Baltimore, MD 21230.

5. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Cincinnati, Inc. is a corporation duly organized and existing under the laws of the state of Ohio, with its principal place of business at 2950 Robertson Avenue, Cincinnati, OH, 45209.

6. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Dallas, Inc. is a corporation duly organized and existing under the laws of the state of Deleware, with its principal place of business at 1021 Main Street, Suite 1150, Houston, TX 77002.

7. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Fullerton, Inc. is a corporation duly organized and existing under the laws of the state of California, with its principal place of business at 9601 Mcallister Freeway, Suite 610, San Antonio, TX 78216.

8. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Jacksonville, LLC is a corporation duly organized and existing under the laws of the state of Delaware, with its principal place of business at 9601 Mcallister Freeway, Suite 610, San Antonio, TX 78216.

9. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Direct Marketing/Kansas City, LLC is a corporation duly organized and existing under the laws of the state of Delaware, with its principal place of business at 9601 Mcallister Freeway, Suite 610, San Antonio, TX 78216.

10. SMS is informed and believes, and on that basis alleges that Defendant Harte-Hanks Print, Inc. is a corporation duly organized and existing under the laws of the state of New Jersey, with its principal place of business at 9601 Mcallister Freeway, Suite 610, San Antonio, TX 78216.

11. SMS is informed and believes, and on that basis alleges that the Defendants identified in Paragraphs 2-10 above (collectively "Harte-Hanks") are interrelated companies that together comprise a leading provider of mail services. These Defendants operate as a unitary business venture and are jointly and severally liable for patent infringement related to mail services provided by any one of them. SMS's right to relief against each of these nine Defendants arises out of the same transaction, occurrence, or series of transactions or occurrences relating to making, using, importing into the United States, offering for sale, or selling mail services that are common to each of the nine Defendants. Additionally, questions of fact that are

common to all nine Defendants will arise in this action, including whether software that is jointly used by all nine Defendants infringes the asserted patents. Therefore, joinder of the nine Defendants identified in Paragraphs 2-10 above is proper under 35 U.S.C. § 299.

12. By way of example only, SMS is informed and believes, and on that basis alleges that Harte-Hanks uses certain software to generate and process various barcodes, including the Intelligent Mail Barcode ("IMb"). The IMb is one of several barcodes used by the United States Postal Service ("USPS"). The IMb is a data-rich barcode that can be applied to a mail object, includes information on the mail object, and can be used to uniquely identify the mail object.

13. While IMB specifications are available from the USPS, SMS is informed and believes, and on that basis alleges that Harte-Hanks is performing infringing acts that are independent of the IMb specifications provided by the USPS. In other words, SMS alleges that the infringing conduct includes conduct that goes above and beyond the conduct required to comply with the IMb specifications provided by the USPS. SMS further alleges that the software used by Harte-Hanks to generate and process IMbs and IMb related data is not being used to comply with the IMb specifications provided by the USPS, but is instead being used to provide certain value-added mail services to their customers, *i.e.*, services that infringe the asserted patents.

14. SMS is informed and believes, and on that basis alleges that the software has no substantial non-infringing uses, and was especially made or adapted for use in an infringement of the asserted patents. Specifically, the software only functions to generate and process IMbs and IMb related data, and only does so in a way that infringes the asserted patents. SMS is informed and believes, and on that basis alleges that the software cannot be used for any other purpose other than infringement.

15. SMS is informed and believes, and on that basis alleges that Harte-Hanks has been aware of the asserted patents and the infringement allegations since at least July 2012, and continues to use its software to infringe the asserted patents. SMS alleges that, to the extent that Harte-Hanks' customers are using the software, or a portion thereof, they are doing so at the direction of Harte-Hanks.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 et seq. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b) in that a substantial part of the events giving rise to the claims occurred in this district and the Defendants have a regular and established practice of business in this district and have committed acts of infringement in this district.

SECURED MAIL SOLUTIONS, LLC

17. SMS is a provider of mail and mail information services and technology, and is the owner of the three patents-in-suit, U.S. Pat. Nos. 7,814,032, 7,818,268 and 8,073,787.

18. The patents-in-suit disclose and claim various systems and methods for processing, verifying and/or authenticating mail identification data. In one embodiment of the claimed inventions, mail identification data is affixed to a mail object and includes (or is linked to) information related to the mail object (*e.g.*, information on the sender of the mail object, the contents of the mail object, etc.). This information can then be used by various individuals or entities (*e.g.*, a mail house, a mail carrier, a recipient, etc.) to ensure that the mail object is secure, and can safely be processed, routed and opened. In fact, during prosecution of U.S. Pat. No. 7,818,268 ("the '268 patent"), the USPTO granted the '268 patent special examination status for disclosing "counter terrorism" technology. According to the USPTO, the '268 patent discloses technology that "reduces the risk of [a] terrorist attack." *See* File History for the '268 patent, Decision on Petition to Make Special (Counter Terrorism), dated October 8, 2003. While the mail identification data claimed in the patents-in-suit can be used to secure mail object, the data can also be used by mail houses to more effectively process and route mail objects.

INFRINGEMENT OF U.S. PATENT NO. 7,814,032

19. SMS repeats and realleges the allegations of the preceding paragraphs as if set forth herein.

20. On October 12, 2010, United States Patent No. 7,814,032 ("the '032 patent") was duly and legally issued for an invention entitled "System and Method for Mail Verification." SMS was assigned the '032 patent and continues to hold all rights and interest in the '032 patent. A true and correct copy of the '032 patent is attached hereto as Exhibit 1.

21. Harte-Hanks has infringed and continues to infringe one or more claims of the '032 patent. Harte-Hanks is liable for infringing the '032 patent under 35 U.S.C. § 271 by at least generating, storing and processing mail identification data as claimed in the patent, and/or contributing to or inducing others in the generation, storage and/or processing of mail identification data as claimed in the patent. This includes, but is not limited to, use of the software identified in Paragraphs 12 and 13 above, and/or contributing to or inducing others (*e.g.*, Harte-Hanks' customers, recipients of mail objects, etc.) to use at least a portion of the software identified in Paragraphs 12 and 13 above.

22. Harte-Hanks has had actual notice of the '032 patent and SMS's infringement contentions since at least July 2012, and, notwithstanding such notice, has continued to willfully infringe, induce infringement of, and contribute to infringement of the '032 patent.

23. Harte-Hanks' acts of infringement have caused damage to SMS, and SMS is entitled to recover from Harte-Hanks the damages sustained by SMS as a result of Harte-Hanks' wrongful acts in an amount subject to proof at trial. Harte-Hanks' infringement of SMS's exclusive rights under the '032 patent will continue to damage SMS, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court.

INFRINGEMENT OF U.S. PATENT NO. 7,818,268

24. SMS repeats and realleges the allegations of the preceding paragraphs as if set forth herein.

25. On October 19, 2010, United States Patent No. 7,818,268 ("the 268 patent") was duly and legally issued for an invention entitled "System and Method for Mail Verification." SMS was assigned the '268 patent and continues to hold all rights and interest in the '268 patent. A true and correct copy of the '268 patent is attached hereto as Exhibit 2.

26. Harte-Hanks has infringed and continues to infringe one or more claims of the '268 patent. Harte-Hanks is liable for infringing the '268 patent under 35 U.S.C. § 271 by at least generating, storing and processing mail identification data as claimed in the patent, and/or contributing to or inducing others in the generation, storage and/or processing of mail identification data as claimed in the patent. This includes, but is not limited to, use of the software identified in Paragraphs 12 and 13 above, and/or contributing to or inducing others (*e.g.*, Harte-Hanks' customers, recipients of mail objects, etc.) to use at least a portion of the software identified in Paragraphs 12 and 13 above.

27. Harte-Hanks has had actual notice of the '268 patent and SMS's infringement contentions since at least July 2012, and, notwithstanding such notice, has continued to willfully infringe, induce infringement of, and contribute to infringement of the '268 patent.

28. Harte-Hanks' acts of infringement have caused damage to SMS, and SMS is entitled to recover from Harte-Hanks the damages sustained by SMS as a result of Harte-Hanks' wrongful acts in an amount subject to proof at trial. Harte-Hanks' infringement of SMS's exclusive rights under the '268 patent will continue to damage SMS, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court.

INFRINGEMENT OF U.S. PATENT NO. 8,073,787

29. SMS repeats and realleges the allegations of the preceding paragraphs as if set forth herein.

30. On December 6, 2011, United States Patent No. 8,073,787 ("the '787 patent") was duly and legally issued for an invention entitled "System and Method for Mail Verification." SMS was assigned the '787 patent and continues to hold all rights and interest in the '787 patent. A true and correct copy of the '787 patent is attached hereto as Exhibit 3.

31. Harte-Hanks has infringed and continues to infringe one or more claims of the '787 patent. Harte-Hanks is liable for infringing the '787 patent under 35 U.S.C. § 271 by at least generating, storing and processing mail identification data as claimed in the patent, and/or contributing to or inducing others in the generation, storage and/or processing of mail

identification data as claimed in the patent. This includes, but is not limited to, use of the software identified in Paragraphs 12 and 13 above, and/or contributing to or inducing others (*e.g.*, Harte-Hanks' customers, recipients of mail objects, etc.) to use at least a portion of the software identified in Paragraphs 12 and 13 above.

32. Harte-Hanks has had actual notice of the '787 patent and SMS's infringement contentions since at least July 2012, and, notwithstanding such notice, has continued to willfully infringe, induce infringement of, and contribute to infringement of the '787 patent.

33. Harte-Hanks' acts of infringement have caused damage to SMS, and SMS is entitled to recover from Harte-Hanks the damages sustained by SMS as a result of Harte-Hanks' wrongful acts in an amount subject to proof at trial. Harte-Hanks' infringement of SMS's exclusive rights under the '787 patent will continue to damage SMS, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court.

JURY DEMAND

34. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, SMS respectfully requests a trial by jury on all issues properly triable by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Secured Mail Solutions, LLC ("SMS") requests entry of judgment in its favor and against Defendants as follows:

a) Declaration that Harte-Hanks has infringed, contributed to the infringement of, or induced infringement of U.S. Patent Nos. 7,814,032, 7,818,268 and 8,073,787.

b) Awarding the damages arising out of Harte-Hanks' infringement of, contribution to the infringement of, or inducement of infringement of U.S. Patent Nos. 7,814,032, 7,818,268 and 8,073,787 to SMS, together with prejudgment and post-judgment interest, in an amount according to proof;

c) Permanently enjoining Harte-Hanks and their respective officers, agents, employees, and those acting in privity with them, from further infringement, including

contributory infringement and/or inducing infringement, of U.S. Patent Nos. 7,814,032, 7,818,268 and 8,073,787, or in the alternative, awarding a royalty for post-judgment infringement;

d) Finding this case to be exceptional, and awarding enhanced damages and attorney's fees to SMS pursuant to 35 U.S.C. §§ 284 and 285 or as otherwise permitted by law; and

e) Awarding such other costs and further relief as the Court may deem just and proper.

Dated: August 22, 2012

BRETT J. WILLIAMSON (S.B. #145235)
bwilliamson@omm.com
O'MELVENY & MYERS LLP
610 Newport Center Drive, 17th Floor
Newport Beach, CA 92660-6429
Telephone: (949) 760-9600
Facsimile: (949) 823-6994

RYAN K. YAGURA (S.B. #197619)
ryagura@omm.com
VISION L. WINTER (S.B. #234172)
vwinter@omm.com
O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000
Facsimile: (213) 430-6407

Attorneys for SECURED MAIL SOLUTIONS, LLC

PROOF OF SERVICE

I, Lynn S. Talab, declare:

I am a resident of the State of California and over the age of eighteen years, and not a party to the within action; my business address is 400 South Hope Street, Los Angeles, CA 90071-2899. On August 22, 2012, I served the within document:

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

☒ by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at Los Angeles, California addressed as set forth below. I am readily familiar with the firm's practice of collecting and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if the postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit;

☐ by causing the document(s) to be emailed or electronically transmitted to the person(s) at the email addresses set forth below, pursuant to a court order or an agreement of the parties to accept service by email or electronic transmission. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful;

on the attached Service List.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on August 22, 2012 at Los Angeles, California.

/s/ Lynn S. Talab
Lynn S. Talab

SERVICE LIST

Counsel for Defendants

Mario Moore
mario.moore@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
5 Park Plaza, Suite 1750
Irvine, CA 92614

Winn Carter, Jr.
wcarter@morganlewis.com
James A. Glenn
jglenn@morganlewis.com
MORGAN, LEWIS & BOCKIUS LLP
1000 Louisiana Street, Suite 4000
Houston, TX 77002

EXHIBIT 1

US007814032B2

(12) **United States Patent**
Fitzsimmons

(10) **Patent No.: US 7,814,032 B2**
(45) **Date of Patent: Oct. 12, 2010**

(54) **SYSTEM AND METHOD FOR MAIL VERIFICATION**

(76) Inventor: **Todd E. Fitzsimmons**, 237 Lindero Ave., Long Beach, CA (US) 90803

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 644 days.

(21) Appl. No.: **11/519,739**

(22) Filed: **Sep. 11, 2006**

(65) **Prior Publication Data**

US 2007/0022060 A1 Jan. 25, 2007

Related U.S. Application Data

(63) Continuation of application No. 10/271,471, filed on Oct. 15, 2002.

(60) Provisional application No. 60/330,031, filed on Oct. 16, 2001.

(51) **Int. Cl.**

G06F 17/00	(2006.01)
G06Q 10/00	(2006.01)
G06Q 20/00	(2006.01)
G07B 17/02	(2006.01)
G06F 21/00	(2006.01)

(52) **U.S. Cl.** **705/401**; 705/1.1; 705/64; 705/402; 705/408; 713/186

(58) **Field of Classification Search** 705/1.1, 705/64, 401, 402, 408; 713/186

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2002/0029152 A1 * 3/2002 Lee et al. 705/1

FOREIGN PATENT DOCUMENTS

JP 2001275159 A * 10/2001
WO WO 01/35348 A1 * 5/2001

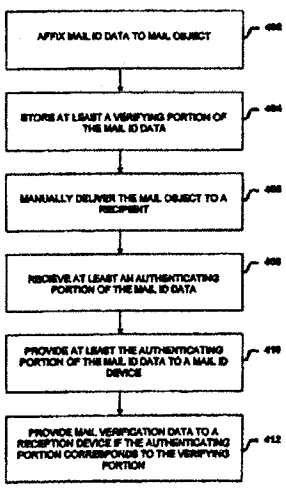
* cited by examiner

Primary Examiner—Fadey S Jabr

(57) **ABSTRACT**

A system and method is provided for transmitting mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In one embodiment of the present invention, a mail verification application is adapted to store at least a verifying portion (e.g., an identifiable code portion, a shipping portion, a recipient portion, etc.) of mail ID data in memory. The mail ID data is then affixed to a mail object. The mail object is then manually delivered to a recipient. At least an authenticating portion of the mail ID data is then provided to a reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion of the mail ID data is authenticated, mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data, securing data, sender data, recipient data, mail-content data, downloadable-product data, sender-web-page data, and/or third-party-web-page data.

22 Claims, 3 Drawing Sheets



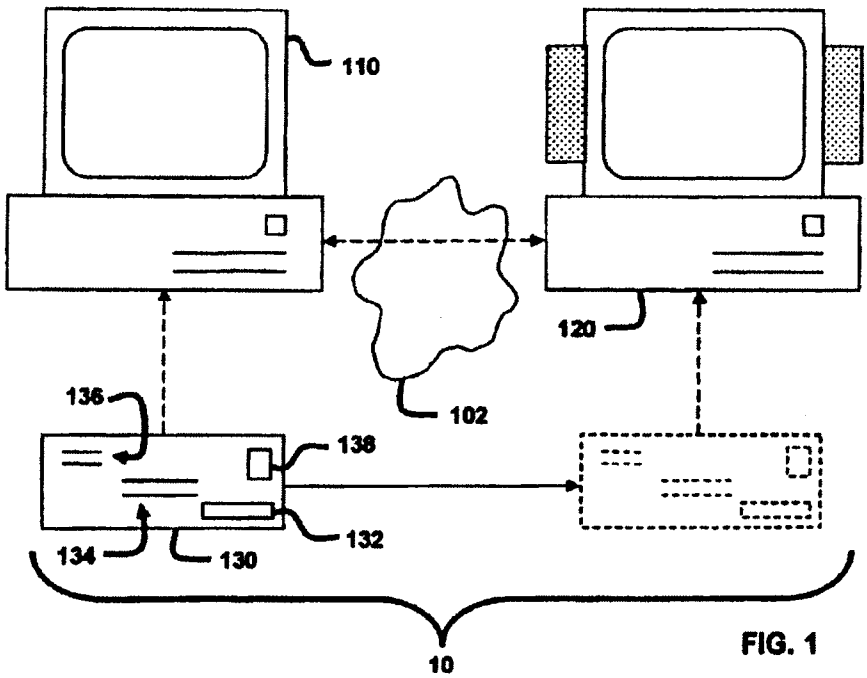


FIG. 1

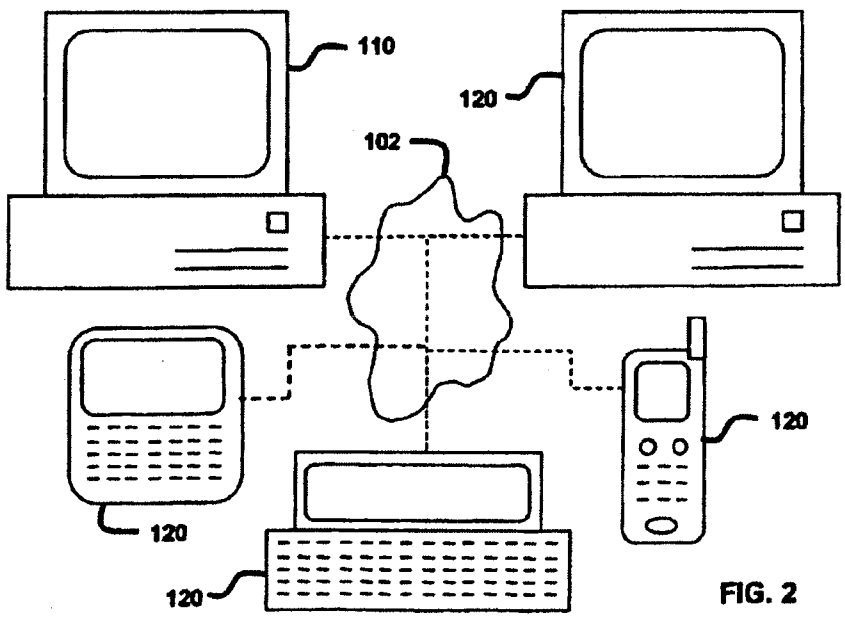


FIG. 2

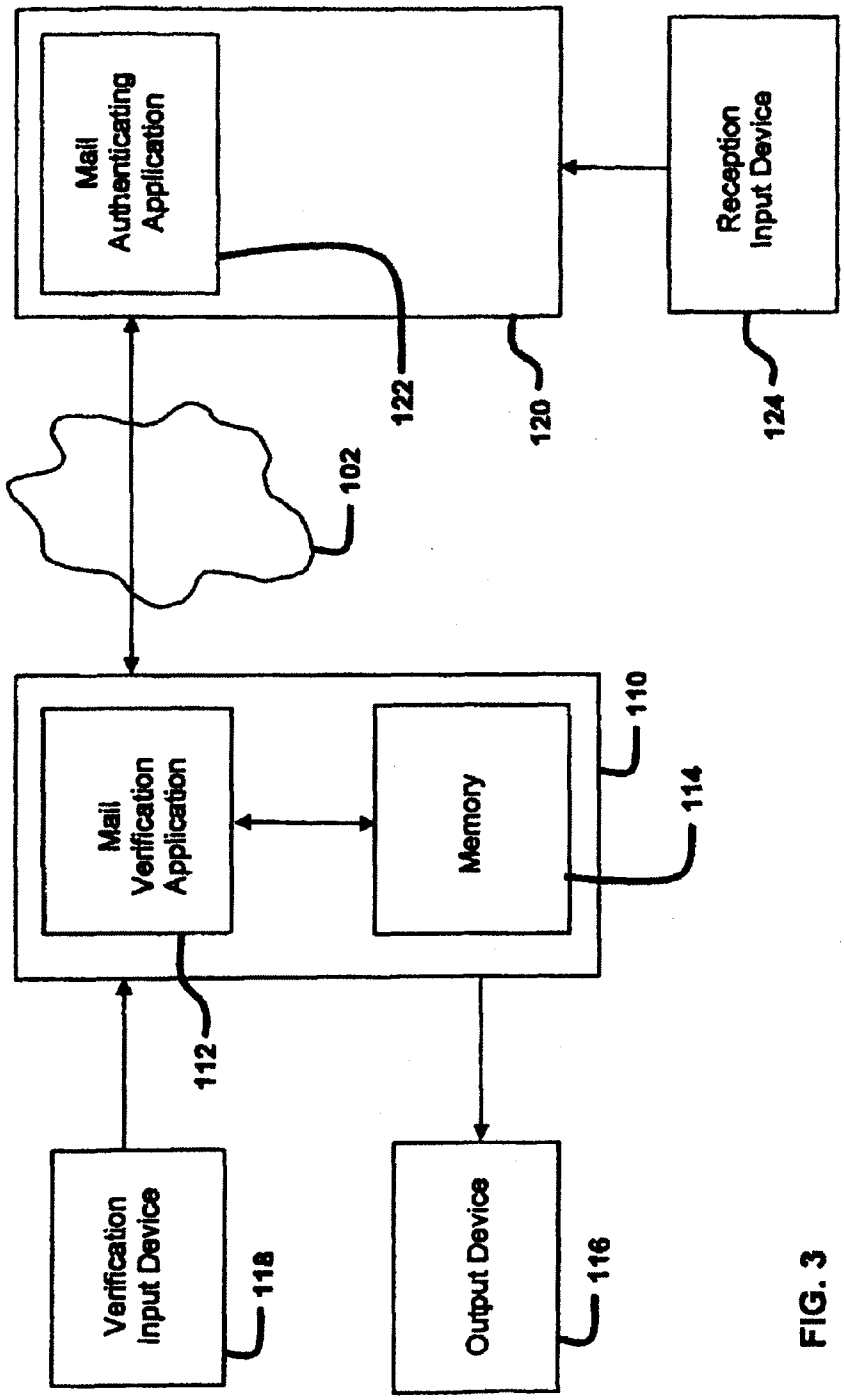

Mail Authenticating Application
Reception Input Device
122
120
124
102
Mail Verification Application
Memory
110
114
112
Verification Input Device
118
Output Device
116

FIG. 3

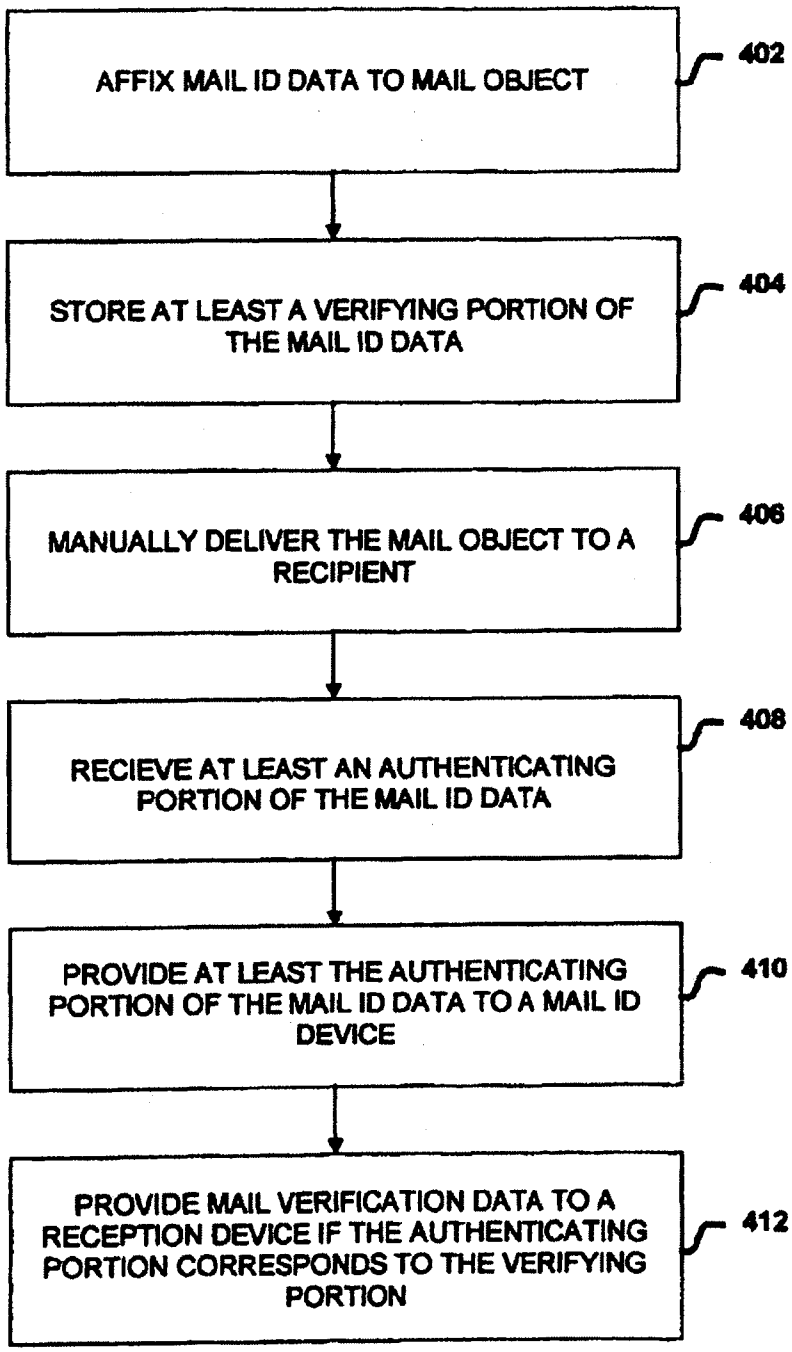

AFFIX MAIL ID DATA TO MAIL OBJECT
402
STORE AT LEAST A VERIFYING PORTION OF THE MAIL ID DATA
404
MANUALLY DELIVER THE MAIL OBJECT TO A RECIPIENT
406
RECIEVE AT LEAST AN AUTHENTICATING PORTION OF THE MAIL ID DATA
408
PROVIDE AT LEAST THE AUTHENTICATING PORTION OF THE MAIL ID DATA TO A MAIL ID DEVICE
410
PROVIDE MAIL VERIFICATION DATA TO A RECEPTION DEVICE IF THE AUTHENTICATING PORTION CORRESPONDS TO THE VERIFYING PORTION
412

FIG. 4

SYSTEM AND METHOD FOR MAIL VERIFICATION

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of U.S. patent application Ser. No. 10/271,471, filed Oct. 15, 2002, which claims the benefit pursuant to 35 U.S.C. §119(e) of U.S. Provisional Patent Application No. 60/330,031 filed Oct. 16, 2001, which applications are specifically incorporated herein, in their entirety, by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to mail verification, and more particularly to a system and method of authenticating at least one mail object by providing at least a portion of mail identification data over a wide area network, such as the Internet, in order to receive mail verification data.

2. Description of Related Art

Currently there are two ways to provided mail objects (e.g., letters, documents, packages, etc.) to an end user; that being electronically (e.g., email, etc.) and through traditional mail services (e.g., U.S. Postal Service, Federal Express, UPS, Courier, etc.). However, because certain mail objects cannot be delivered electronically (either because its impossible or impractical), they are delivered using traditional mail services.

There are several problems with delivering mail objects through traditional mail services. First, the mail object is typically secured inside packaging (e.g., envelops, boxes, etc.) before it is provided to the mail service. Thus, neither the mail service nor the recipient is aware of the contents of the package until such package is opened by the recipient. This creates a problem in that hazardous mail objects (i.e., Anthrax, explosives, etc.) are not detected until they are opened by the recipient, thus exposing the recipient to the hazardous material. It also creates a problem in that mail objects (in general) are not known until they are opened by the recipient, thus making it difficult for the recipient (or his designee) to properly screen, sort or avoid certain mail objects (e.g., offensive mail, annoying mail, etc).

Second, a manually delivered mail object is limited to a one-way production of a finite set of information and/or products. This becomes problematic when the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.). Finally, contents that can be delivered electronically (e.g., advertisements, software, etc.) are often included in mail objects that are delivered via traditional mail services. The drawback with this is that it increases the cost associated with producing and/or delivering the mail object and increase the size of the mail object. For at least these reasons, a need exists in the industry for a system and method of providing mail verification data in response to receiving mail ID data over a wide area network, such as the Internet.

SUMMARY OF THE INVENTION

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. Preferred embodiments of the present invention operate in accordance with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. Specifically, the mail verification application is adapted to store at least a verifying portion of mail ID data in memory. In one embodiment of the present invention, the verifying portion of the mail ID data includes an identifiable code portion (e.g., an alpha code, a numeric code, an alphanumeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.) and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail ID data is then affixed to a mail object. The mail object, which may further include a mail-to-address, a return-mail-address, and/or postage, is then manually delivered to a recipient. In one embodiment of the present invention, the mail ID data further includes mail-to-address data, return-mail-address data, and/or postage data.

At least an authenticating portion of the mail ID data is then provided to the reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (indicating that the mail ID data has been authenticated), securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating the intended recipient of the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page information, third party advertisements, etc).

In one embodiment of the present invention, the mail ID device further includes an input device adapted to provide at least a verifying portion of the mail ID data to the mail verification application and/or an output device adapted to affix the mail ID data on the mail object. In another embodiment of the present invention, the reception device includes an input device for receiving at least an authenticating portion of the mail ID data from the mail object and/or a mail authenticating application adapted to receive at least the authenticating portion of the mail ID data from the input device and provide at least the authenticating portion of the mail ID data to the mail ID device. In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient of the mail object, thus interacting with the reception device to receive mail verification data.

A more complete understanding of the system and method for providing mail verification data in response to receiving at least a portion of mail ID data will be afforded to those skilled in the art, as well as a realization of additional advantages and objects thereof, by a consideration of the following detailed description of the preferred embodiment. Reference will be made to the appended sheets of drawings which will first be described briefly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates one embodiment of the mail verification system.

FIG. **2** illustrates a mail ID device communicating with a plurality of reception devices over a wide area network, such as the Internet.

FIG. **3** illustrates one embodiment of the mail ID device and the reception device depicted in FIG. **1**.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of mail ID data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In the detailed description that follows, like element numerals are used to describe like elements illustrated in one or more figures.

Preferred embodiments of the present invention operate in accordance with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. FIG. **1** illustrates one embodiment of the mail verification system **10**, which includes a mail ID device **110** and a reception device **120** communicating through a wide area network **102**, such as the Internet. It should be appreciate, as depicted in FIG. **2**, that the reception device(s) **120** includes, but is not limited to, personal computers, set top boxes, personal digital assistances (PDAs), mobile phones, land-line phones, televisions, bar code readers, and all other physically and wirelessly connected reception devices generally known to those skilled in the art. It should further be appreciated that the number of reception devices **120** depicted in FIGS. **1** and **2** are merely to illustrate how the present invention operates, and are not intended to further limit the present invention.

As shown in FIG. **3**, the mail ID device **110** further includes a mail verification application **112** and a memory **114**. The mail verification application **112** is adapted to store at least a portion (i.e., a verifying portion) of mail ID data in the memory **114**, receive at least a portion (i.e., an authenticating portion) of mail ID data from the reception device **120**, and provide mail verification data if the portion of the mail ID data received from the reception device **120** is authenticated. It should be appreciated that the mail verification application **112** may further be adapted to generate the mail ID data and provide it to an external device (e.g., a printer, etc.) or receive at least a verifying portion of the mail ID data from an external device (e.g., a scanner, etc.). It should also be appreciated that the mail verification application **112** may exist as a single application, or as multiple applications (locally and/or remotely stored) that operate together to perform the verification functions as described herein. It should further be appreciated that the location of the memory device **114** depicted in FIG. **3** is not intended to further limit the present invention. Thus, a memory device that is, for example, external to the mail ID device **110** is within the spirit and scope of the present invention.

Referring back to FIG. **1**, where the dashed arrows indicate data transactions and the solid arrow indicates physical movement, mail ID data **132** is affixed to a mail object **130** (as used in its broader sense to encompass the packaging that surrounds the content). It should be appreciated that mail ID data can be encoded/encrypted (e.g., using bar code data, digital data, etc.) to prevent fraudulent usage. It should further be appreciated that affixing the mail ID data **132** on the mail object **130** includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object **130** or printing/storing the mail ID data **132** on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object **130**. It should also be appreciated that the location of the mail ID data **132** on the mail object **130** in FIG. **1** is merely to exemplify how the invention operates, and is not intended to further limit the present invention. Thus, affixing the mail ID data **132** in some other location, such as over the sealing flap of an envelope, is within the spirit and scope of this invention.

At least a portion (i.e., a verifying portion) of the mail ID data **132** (either before or after the mail ID data is affixed) is stored in the mail ID device **110**, or more particular (as shown in FIG. **3**) in a memory **114** located within the mail ID device **110**. Specifically, the mail verification application **112** either receives or generates at least the verifying portion of the mail ID data **132**. The verifying portion is then stored in the memory **114**. In one embodiment of the present invention, the verifying portion of the mail ID data includes a identifiable code portion (e.g., an alpha code, a numeric code, and alpha-numeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.), and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail object **130**, which may further include a mail-to-address **134**, a return-mail-address **136**, and/or postage **138**, can then be manually delivered to a recipient. It should be appreciated that the mail ID data **132** can also be encoded (e.g., in a bar code, etc.) to include mail-to-address data, return-mail-address data, and/or postage data. In other words, for example, mail ID data could be encoded to include both coded data and postage-account data.

Once the recipient (or their designee) receives the mail object **130**, at least an authenticating portion of the mail ID data **132** is provided to the reception device **120**. The reception device **120**, which communicates with the mail ID device **110** over a wide area network **102**, transmits at least the authenticating portion of the mail identification data to the mail verification application **112** operating on the mail ID device **110**. The mail verification application **112** then compares the authenticating portion of the mail ID data with the verifying portion stored in memory **114**. If the received portion is authenticated, or corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device **120**.

In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (e.g., image data, audio data, etc.) indicating that the mail ID data has been authenticated. This would allow, for example, the reception device **120** to produce at least one authenticating image on a display and/or perform at least one authenticating sound on a speaker. In another embodiment of the present invention at least a portion of the mail verification data includes securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating who is to receive the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page data, third party advertisements, etc).

In another embodiment of the present invention, the mail ID device and/or the reception device further include an input device (e.g., **118**, **124**) adapted to receive at least a portion of the mail ID data. It should be appreciated that that the input devices depicted and discussed herein (e.g., **118**, **124**) include, but are not limited to, scanners (e.g., bar code scan-

ners, etc.), keyboards, RFID readers, smart card readers, IC readers, and all other input devices generally known to those skilled in the art.

In another embodiment of the present invention, the mail ID device further includes an output device **116** adapted to affix (e.g., print, store, etc.) the mail ID data on the mail object. It should be appreciated that affixing the mail ID data on the mail object includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object or printing/storing the mail ID data on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object. It should further be appreciated that the output device depicted and described herein (e.g., **116**) includes, but is not limited to, printers, data storage device (e.g., device capable of storing data on ICs, smart cards, RFID tags, etc.), and all other output devices generally known to those skilled in the art.

In another embodiment of the present invention, as shown in FIG. **3**, the reception device **120** further includes a mail authenticating application **122** adapted to receive at least the authenticating portion of the mail ID data from the input device **124** and provide at least the authenticating portion of the mail ID data to the mail ID device. It should be appreciated that the mail authenticating application **122** may exist as a single application, or as: multiple applications (locally and/or remotely stored) that operate together to perform the authenticating functions as described herein.

In one embodiment of the present invention, the mail ID data further includes software-booting data adapted to boot the mail authenticating application, an email application and/or a browser application. Either one of these applications could then be used to provide at least an authenticating portion of said mail ID data to said mail ID device, provide additional information to said mail ID device (or the sender of the mail object), and/or receive additional information from either the mail ID device, the sender of the mail object, or a third-party. In another embodiment, the mail verification data further includes software-booting data adapted to boot an email application and/or a browser application. Either one of these applications could then be used to provide additional information to the mail ID device and/or receive additional information from either the mail ID device, the sender of the mail object, or a third party.

In another embodiment of the invention, the reception device **120**, or more particularly the mail authenticating application **122** is adapted to provide a reply email to the mail ID device **130** or the sender of the mail object. This reply email may either be sent automatically, to acknowledge the reception of the mail ID data and/or mail verification data, or manually, to allow the recipient to communicate with the mail ID device and/or sender of the mail object. In another embodiment of the invention the mail verification application **112** is adapted to provide the mail verification data to the reception device **120** via an email.

In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient (as defined by this application) of the mail object **130**, thus interacting with the reception device **120** to receive mail verification data. If mail is authenticated (or approved in the case of screening), the mail object **130** is forwarded on to the actual intended recipient.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of the mail ID data. Specifically, in step **402** mail ID data is affixed to a mail object. At step **404**, a verifying portion of the mail ID data is stored in a memory device. The mail object is then delivered to its recipient (or designee) at step **406**. At step **408**, a reception device receives at least an authenticating portion of the mail ID data. The reception device then provides at least the authenticating portion to a mail ID device at step **410**. If the authenticating portion of the mail ID data corresponds to the verifying portion of the mail ID data, then mail verification data is provided to the reception device at step **412**. It should be appreciated that storing the verifying portion of the mail ID data before the mail ID data is affixed to the mail object is within the spirit and scope of the present invention.

Having thus described multiple embodiments of a system and method of providing mail verification data in response to receiving mail ID data, it should be apparent to those skilled in the art that certain advantages of the system have been achieved. It should also be appreciated that various modifications, adaptations, and alternative embodiments thereof may be made within the scope and spirit of the present invention. The invention is further defined by the following claims.

What is claimed is:

1. A method for using a single barcode to verify the authenticity of and identify a sender of a physical mail object that is being sent from said sender to a recipient via a mail carrier, comprising:

a sender of a physical mail object generating a unique identifier, wherein said unique identifier comprises a numeric value, can be used by said sender to identify said physical mail object, and is distinguishable from a second unique identifier that can be used by said sender to identify a second physical mail object that is being sent from said sender to said recipient via said mail carrier;

encoding at least said unique identifier, sender data and recipient data into a single barcode, wherein said sender data identifies said sender of said physical mail object and said recipient data identifies a recipient of said physical mail object;

storing at least a portion of said encoded data in a database, said portion comprising at least said unique identifier, said sender data and said recipient data;

printing said single barcode on said physical mail object;

submitting said physical mail object to a postal carrier;

scanning by a scanner said single barcode to acquire said encoded data; and

comparing by a computer at least a portion of said encoded data to data stored in said database to verify the authenticity of said physical mail object, wherein said at least a portion of said encoded data comprises at least said unique identifier, said sender data and said recipient data and can be used by said postal carrier to identify said sender of said physical mail object.

2. The method of claim **1**, further comprising the step of sending information pertaining to said physical mail object electronically to said sender, wherein at least a portion of said information indicates that said physical mail object has been received by said mail carrier.

3. The method of claim **1**, wherein said step of encoding at least said unique identifier, sender data and recipient data into a single barcode further comprises encoding at least said unique identifier, sender data, recipient data and shipping data into a single barcode, wherein said shipping data identifies at least a particular method of shipping said physical mail object from said sender to said recipient.

4. The method of claim **1**, wherein said step of storing at least a portion of said encoded data in a database further comprises storing data in said database that can be used to

identify at least one shipping location of said physical mail object and at least one ship date of said physical mail object.

5. The method of claim 1, wherein said step of comparing at least a portion of said encoded data with data stored in said database further comprises (1) delivering said physical mail object directly to said recipient if there is correspondence between said at least a portion of said encoded data and data stored in said database and (2) not delivering said physical mail object directly to said recipient if there is no correspondence between said at least a portion of said encoded data and data stored in said database.

6. The method of claim 2, wherein said step of sending information pertaining to said physical mail object electronically to said sender further comprises sending an email to said sender, wherein said email includes said information.

7. The method of claim 1, wherein said step of storing at least a portion of said encoded data in a database further comprises storing at least a portion of said encoded data in a database that is not maintained by said sender.

8. The method of claim 1, wherein said recipient data identifies said recipient by identifying the destination of said physical mail object.

9. The method of claim 1, wherein said sender data identifies said sender by identifying the origin of said physical mail object.

10. The method of claim 1, wherein said step of submitting said physical mail object to a postal carrier further comprises submitting said physical mail object to the United States Postal Service.

11. The method of claim 1, wherein said step of comparing at least a portion of said encoded data to data stored in said database to verify the authenticity of said physical mail object further comprises determining of there is correspondence between said at least a portion of said encoded data and said data stored in said database.

12. The method of claim 3, wherein said step of comparing at least a portion of said encoded data to data stored in said database further comprising comparing at least said unique identifier, sender data, recipient data and shipping data to data stored in said database.

13. A method for using a single barcode to verify the authenticity of and identify ef a sender of a physical mail object that is being sent from said sender to a recipient via a mail carrier, comprising:

a sender of a physical mail object generating a unique identifier, wherein said unique identifier comprises a numeric value, can be used by said sender to identify said physical mail object, and is distinguishable from a second unique identifier that can be used by said sender to identify a second physical mail object sent from said sender to said recipient via said mail carrier;

encoding at least said unique identifier, sender data, recipient data and shipping method data into a single barcode, wherein said sender data can be used to identify said sender of said physical mail object and said recipient data can be used to identify a recipient of said physical mail object;

storing at least a portion of said encoded data in a database, said portion comprising at least said unique identifier, said sender data and said shipping method data;

printing said single barcode on said physical mail object;

submitting said physical mail object to a postal carrier;

scanning by a scanner said single barcode to acquire said encoded data; and

comparing by a computer at least a portion of said encoded data to data stored in said database to verify the authenticity of said physical mail object, wherein said at least a portion of said encoded data comprises at least said unique identifier, said sender data and said shipping method data and can be used by said postal carrier to identify said sender of said physical mail object.

14. The method of claim 13, further comprising the step of sending information pertaining to said physical mail object electronically to said sender, wherein at least a portion of said information indicates that said physical mail object has been received by said mail carrier.

15. The method of claim 13, wherein said step of storing at least a portion of said encoded data in a database further comprises storing data in said database that can be used to identify at least one shipping location of said physical mail object and at least one ship date of said physical mail object.

16. The method of claim 13, wherein said step of comparing at least a portion of said encoded data with data stored in said database further comprises (1) delivering said physical mail object directly to said recipient if there is correspondence between said at least a portion of said encoded data and data stored in said database and (2) not delivering said physical mail object directly to said recipient if there is no correspondence between said at least a portion of said encoded data and data stored in said database.

17. The method of claim 14, wherein said step of sending information pertaining to said physical mail object electronically to said sender further comprises sending an email to said sender, wherein said email includes said information.

18. The method of claim 13, wherein said step of storing at least a portion of said encoded data in a database further comprises storing at least a portion of said encoded data in a database that is not maintained by said sender.

19. The method of claim 13, wherein said recipient data identifies said recipient by identifying the destination of said physical mail object.

20. The method of claim 13, wherein said sender data identifies said sender by identifying the origin of said physical mail object.

21. The method of claim 13, wherein said step of submitting said physical mail object to a postal carrier further comprises submitting said physical mail object to the United States Postal Service.

22. The method of claim 13, wherein said step of comparing at least a portion of said encoded data to data stored in said database to verify the authenticity of said physical mail object further comprises determining of there is correspondence between said at least a portion of said encoded data and said data stored in said database.

* * * * *

EXHIBIT 2

US007818268B2

(12) **United States Patent**
Fitzsimmons

(10) **Patent No.: US 7,818,268 B2**
(45) **Date of Patent: Oct. 19, 2010**

(54) **SYSTEM AND METHOD FOR MAIL VERIFICATION**

(76) Inventor: **Todd E. Fitzsimmons**, 237 Lindero Ave., Long Beach, CA (US) 90803

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1290 days.

(21) Appl. No.: **10/271,471**

(22) Filed: **Oct. 15, 2002**

(65) **Prior Publication Data**

US 2003/0140014 A1 Jul. 24, 2003

Related U.S. Application Data

(60) Provisional application No. 60/330,031, filed on Oct. 16, 2001.

(51) **Int. Cl.**

G06F 17/00	(2006.01)
G06Q 10/00	(2006.01)
G06Q 20/00	(2006.01)
G07B 17/02	(2006.01)
G06F 21/00	(2006.01)

(52) **U.S. Cl.** **705/401**; 705/1.1; 705/64; 705/402; 705/408; 713/186

(58) **Field of Classification Search** 705/1, 705/28, 29, 1.1, 64, 401–402, 408; 713/186
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,558,318	A *	12/1985	Katz et al.	340/5.86
5,043,908	A *	8/1991	Manduley et al.	700/227
5,684,705	A *	11/1997	Herbert	705/401
5,963,927	A *	10/1999	Herbert	705/401
5,984,366	A *	11/1999	Priddy	283/72

(Continued)

FOREIGN PATENT DOCUMENTS

JP 09-99931 * 4/1997

(Continued)

OTHER PUBLICATIONS

Fales: "Exciting times for new developments in tracking systems. (Automatic Identification)"; Industrial Engineering, May 1992, vol. 24, No. 5, p. 14.*

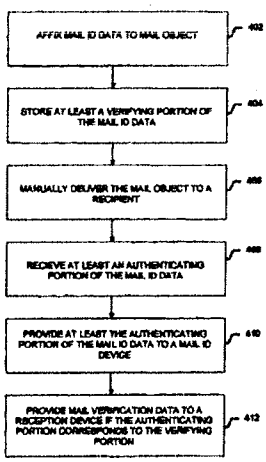
(Continued)

Primary Examiner – Fadey S Jabr

(57) **ABSTRACT**

A system and method is provided for transmitting mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In one embodiment of the present invention, a mail verification application is adapted to store at least a verifying portion (e.g., an identifiable code portion, a shipping portion, a recipient portion, etc.) of mail ID data in memory. The mail ID data is then affixed to a mail object. The mail object is then manually delivered to a recipient. At least an authenticating portion of the mail ID data is then provided to a reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion of the mail ID data is authenticated, mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data, securing data, sender data, recipient data, mail-content data, downloadable-product data, sender-web-page data, and/or third-party-web-page data.

56 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

6,260,029	B1 *	7/2001	Critelli	705/408
6,289,323	B1 *	9/2001	Gordon et al.	705/40
6,510,992	B2 *	1/2003	Wells et al.	235/385
6,539,360	B1 *	3/2003	Kadaba	705/28
6,810,408	B1 *	10/2004	Bates et al.	709/200
7,200,753	B1 *	4/2007	Shinzaki et al.	713/182
7,305,104	B2 *	12/2007	Carr et al.	382/100
2002/0029152	A1 *	3/2002	Lee et al.	705/1
2002/0083022	A1 *	6/2002	Algazi	705/408
2003/0004830	A1 *	1/2003	Frederick	705/26
2003/0101143	A1 *	5/2003	Montgomery et al.	705/62
2003/0101148	A1 *	5/2003	Montgomery et al.	705/404
2003/0102374	A1 *	6/2003	Wojdyla et al.	235/385
2003/0118191	A1 *	6/2003	Wang et al.	380/285
2003/0141358	A1 *	7/2003	Hudson et al.	235/375
2003/0177095	A1 *	9/2003	Zorab et al.	705/50

FOREIGN PATENT DOCUMENTS

JP	2001275159	A *	10/2001
JP	2002-284239	*	10/2002
WO	WO 96/03286	*	2/1996
WO	WO 96/13015	A2 *	5/1996
WO	WO 01/35348	A1 *	5/2001

OTHER PUBLICATIONS

Haskin: "FedEx Ship lets you track packages from your desktop. (Federal Express)(First Looks)(Software Review)(Evaluation)(Brief Article)", PC Magazine, May 16, 1995, vol. 14, No. 9, p. 54.*
Giusti, Christopher, "Mail Center Secuity", Security Management, Nov. 1998, pp. 1-10.*

* cited by examiner

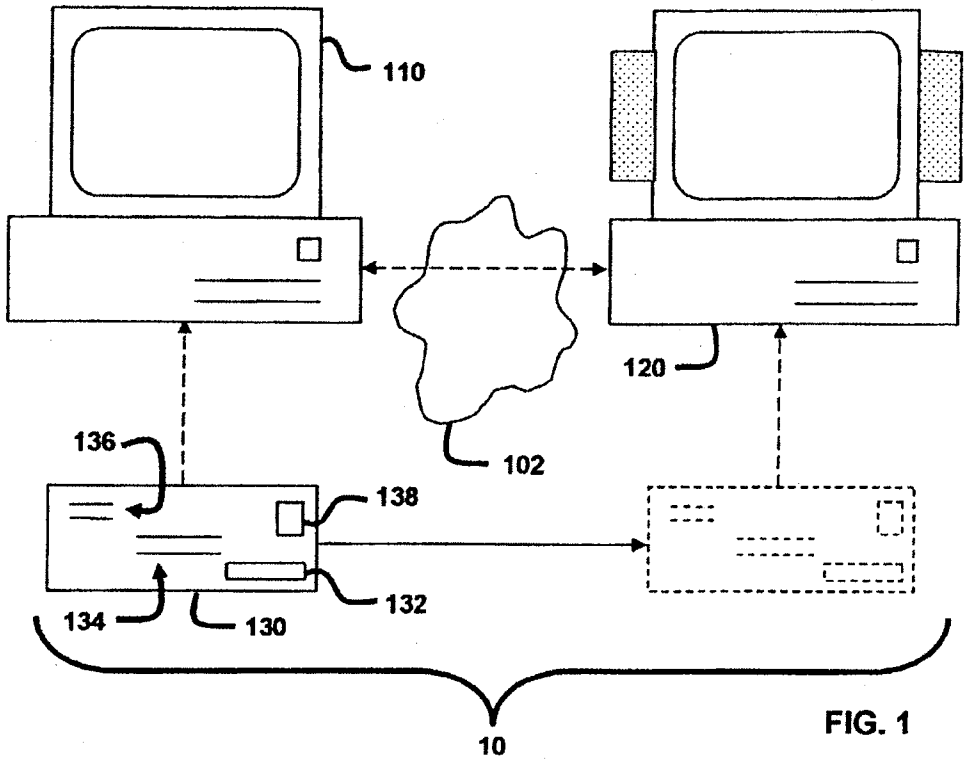


FIG. 1

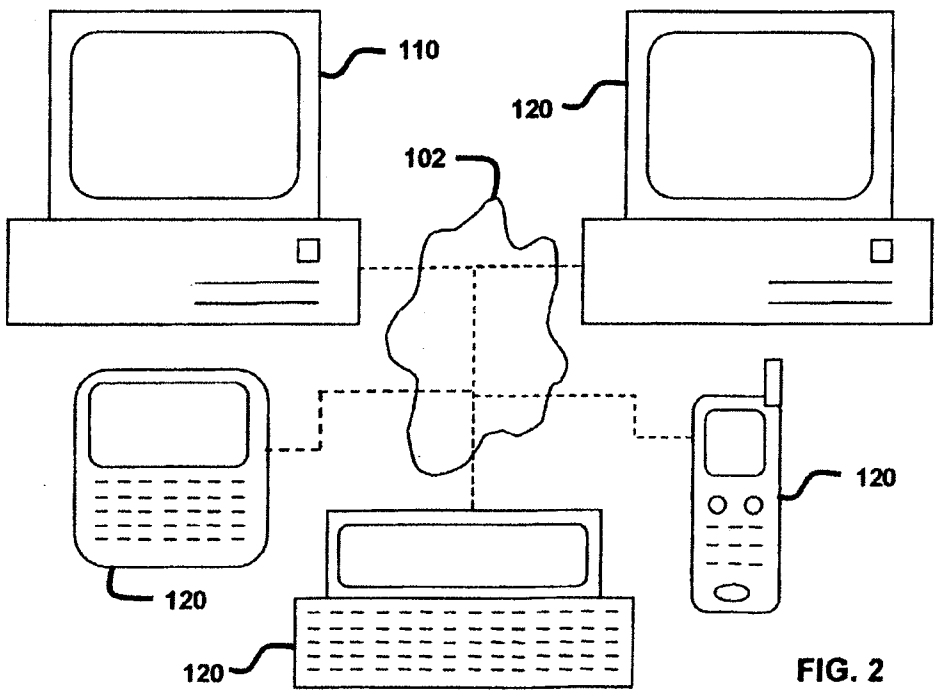


FIG. 2

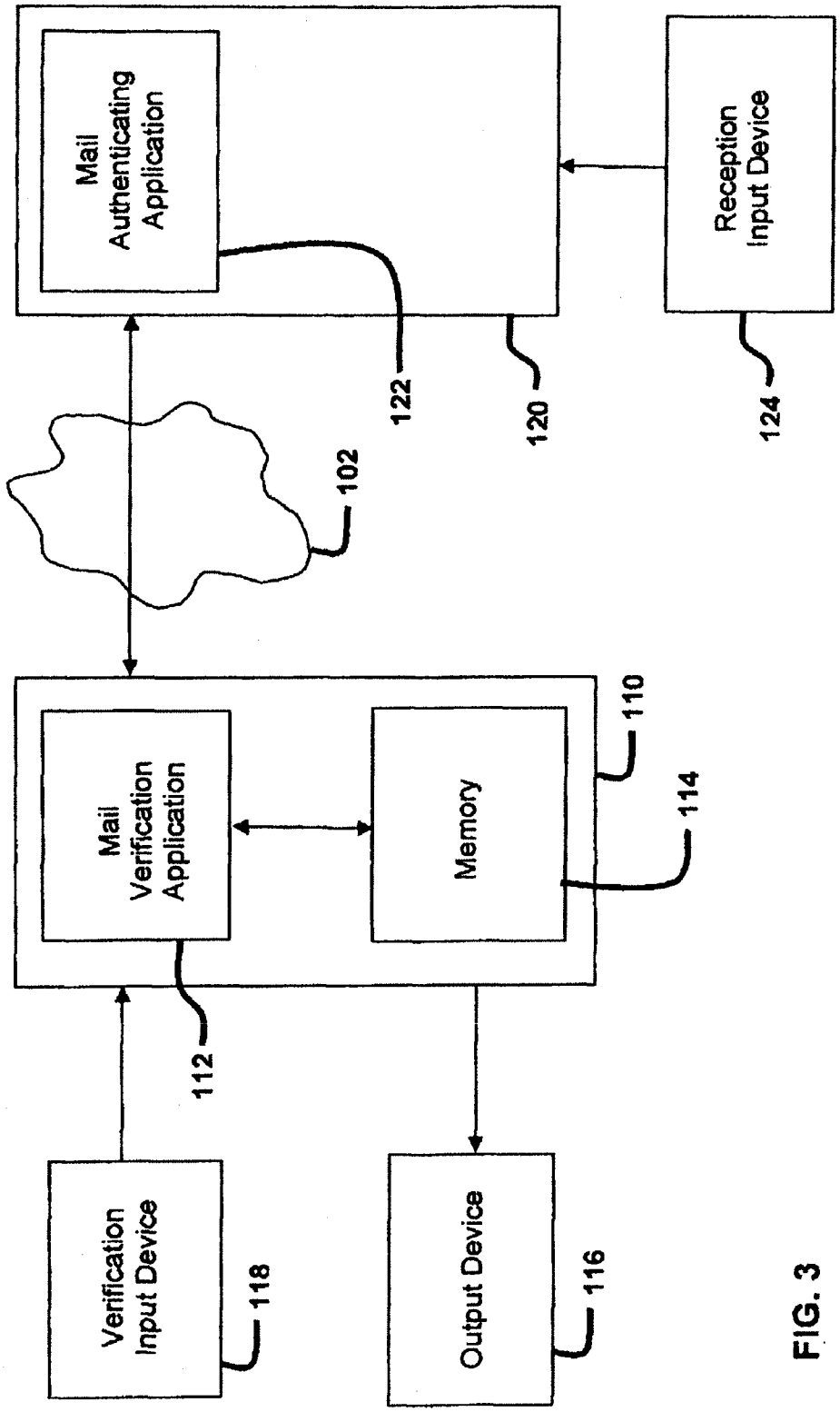

Mail Authenticating Application
Reception Input Device
122
120
124
102
Mail Verification Application
Memory
110
114
112
Verification Input Device
118
Output Device
116

FIG. 3

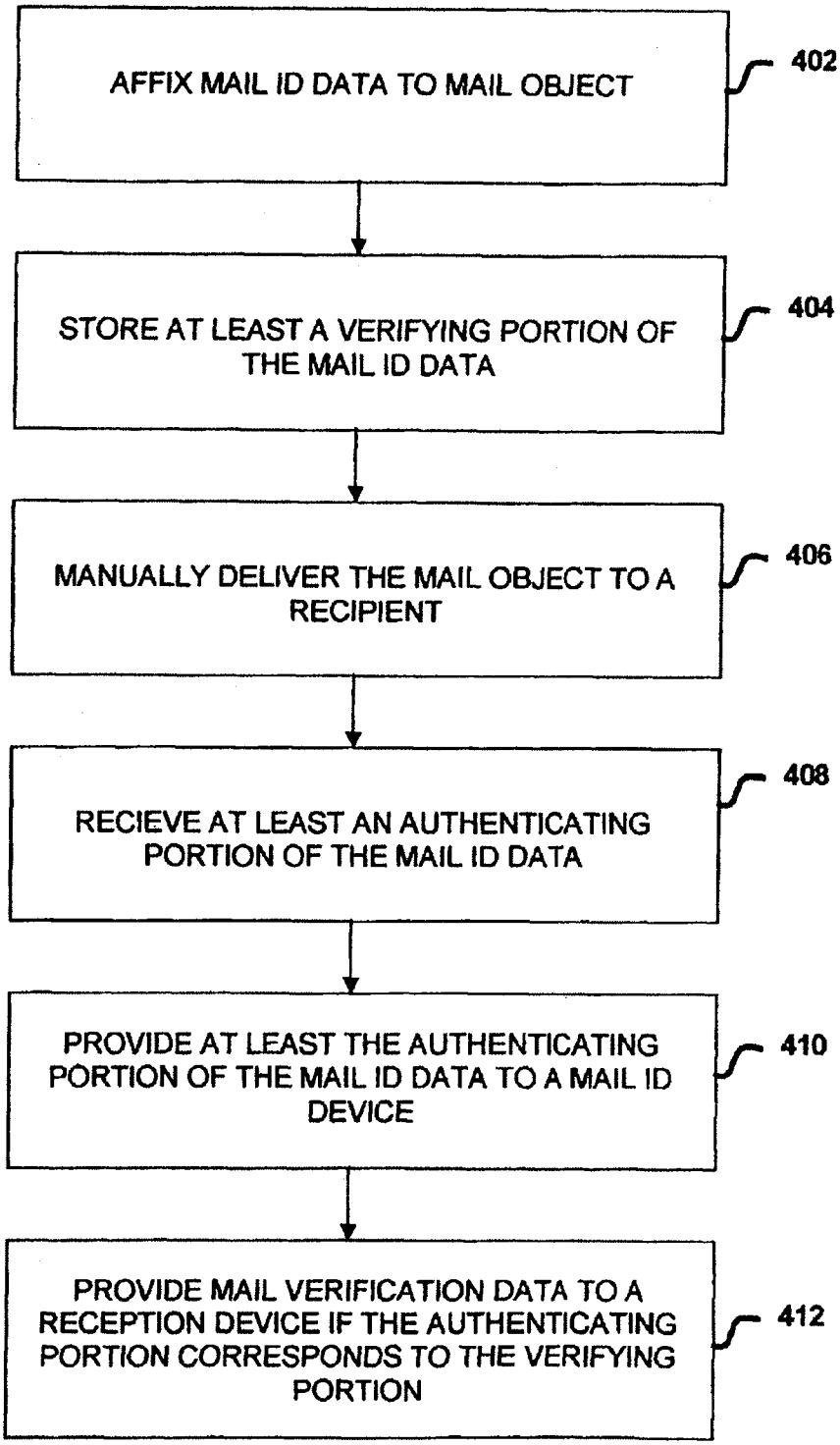

AFFIX MAIL ID DATA TO MAIL OBJECT
402
STORE AT LEAST A VERIFYING PORTION OF THE MAIL ID DATA
404
MANUALLY DELIVER THE MAIL OBJECT TO A RECIPIENT
406
RECIEVE AT LEAST AN AUTHENTICATING PORTION OF THE MAIL ID DATA
408
PROVIDE AT LEAST THE AUTHENTICATING PORTION OF THE MAIL ID DATA TO A MAIL ID DEVICE
410
PROVIDE MAIL VERIFICATION DATA TO A RECEPTION DEVICE IF THE AUTHENTICATING PORTION CORRESPONDS TO THE VERIFYING PORTION
412

FIG. 4

SYSTEM AND METHOD FOR MAIL VERIFICATION

CROSS-REFERENCE TO RELATED APPLICATION

This application claims benefit pursuant to 35 U.S.C. §119(e) of U.S. Provisional Application No. 60/330,031 filed Oct. 16, 2001, which application is specifically incorporated herein, in its entirety, by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to mail verification, and more particularly to a system and method of authenticating at least one mail object by providing at least a portion of mail identification data over a wide area network, such as the Internet, in order to receive mail verification data.

2. Description of Related Art

Currently there are two ways to provided mail objects (e.g., letters, documents, packages, etc.) to an end user; that being electronically (e.g., email, etc.) and through traditional mail services (e.g., U.S. Postal Service, Federal Express, UPS, Courier, etc.). However, because certain mail objects cannot be delivered electronically (either because its impossible or impractical), they are delivered using traditional mail services.

There are several problems with delivering mail objects through traditional mail services. First, the mail object is typically secured inside packaging (e.g., envelops, boxes, etc.) before it is provided to the mail service. Thus, neither the mail service nor the recipient is aware of the contents of the package until such package is opened by the recipient. This creates a problem in that hazardous mail objects (i.e., Anthrax, explosives, etc.) are not detected until they are opened by the recipient, thus exposing the recipient to the hazardous material. It also creates a problem in that mail objects (in general) are not known until they are opened by the recipient, thus making it difficult for the recipient (or his designee) to properly screen, sort or avoid certain mail objects (e.g., offensive mail, annoying mail, etc).

Second, a manually delivered mail object is limited to a one-way production of a finite set of information and/or products. This becomes problematic when the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.). Finally, contents that can be delivered electronically (e.g., advertisements, software, etc.) are often included in mail objects that are delivered via traditional mail services. The drawback with this is that it increases the cost associated with producing and/or delivering the mail object and increase the size of the mail object. For at least these reasons, a need exists in the industry for a system and method of providing mail verification data in response to receiving mail ID data over a wide area network, such as the Internet.

SUMMARY OF THE INVENTION

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. Preferred embodiments of the present invention operate in accordance with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. Specifically, the mail verification application is adapted to store at least a verifying portion of mail ID data in memory. In one embodiment of the present invention, the verifying portion of the mail ID data includes an identifiable code portion (e.g., an alpha code, a numeric code, an alphanumeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.) and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail ID data is then affixed to a mail object. The mail object, which may further include a mail-to-address, a return-mail-address, and/or postage, is then manually delivered to a recipient. In one embodiment of the present invention, the mail ID data further includes mail-to-address data, return-mail-address data, and/or postage data.

At least an authenticating portion of the mail ID data is then provided to the reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (indicating that the mail ID data has been authenticated), securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating the intended recipient of the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page information, third party advertisements, etc).

In one embodiment of the present invention, the mail ID device further includes an input device adapted to provide at least a verifying portion of the mail ID data to the mail verification application and/or an output device adapted to affix the mail ID data on the mail object. In another embodiment of the present invention, the reception device includes an input device for receiving at least an authenticating portion of the mail ID data from the mail object and/or a mail authenticating application adapted to receive at least the authenticating portion of the mail ID data from the input device and provide at least the authenticating portion of the mail ID data to the mail ID device. In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient of the mail object, thus interacting with the reception device to receive mail verification data.

A more complete understanding of the system and method for providing mail verification data in response to receiving at least a portion of mail ID data will be afforded to those skilled in the art, as well as a realization of additional advantages and objects thereof, by a consideration of the following detailed description of the preferred embodiment. Reference will be made to the appended sheets of drawings which will first be described briefly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates one embodiment of the mail verification system.

FIG. **2** illustrates a mail ID device communicating with a plurality of reception devices over a wide area network, such as the Internet.

FIG. **3** illustrates one embodiment of the mail ID device and the reception device depicted in FIG. **1**.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of mail ID data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In the detailed description that follows, like element numerals are used to describe like elements illustrated in one or more figures.

Preferred embodiments of the present invention operate in accordance with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. FIG. **1** illustrates one embodiment of the mail verification system **10**, which includes a mail ID device **110** and a reception device **120** communicating through a wide area network **102**, such as the Internet. It should be appreciate, as depicted in FIG. **2**, that the reception device(s) **120** includes, but is not limited to, personal computers, set top boxes, personal digital assistances (PDAs), mobile phones, land-line phones, televisions, bar code readers, and all other physically and wirelessly connected reception devices generally known to those skilled in the art. It should further be appreciated that the number of reception devices **120** depicted in FIGS. **1** and **2** are merely to illustrate how the present invention operates, and are not intended to further limit the present invention.

As shown in FIG. **3**, the mail ID device **110** further includes a mail verification application **112** and a memory **114**. The mail verification application **112** is adapted to store at least a portion (i.e., a verifying portion) of mail ID data in the memory **114**, receive at least a portion (i.e., an authenticating portion) of mail ID data from the reception device **120**, and provide mail verification data if the portion of the mail ID data received from the reception device **120** is authenticated. It should be appreciated that the mail verification application **112** may further be adapted to generate the mail ID data and provide it to an external device (e.g., a printer, etc.) or receive at least a verifying portion of the mail ID data from an external device (e.g., a scanner, etc.). It should also be appreciated that the mail verification application **112** may exist as a single application, or as multiple applications (locally and/or remotely stored) that operate together to perform the verification functions as described herein. It should further be appreciated that the location of the memory device **114** depicted in FIG. **3** is not intended to further limit the present invention. Thus, a memory device that is, for example, external to the mail ID device **110** is within the spirit and scope of the present invention.

Referring back to FIG. **1**, where the dashed arrows indicate data transactions and the solid arrow indicates physical movement, mail ID data **132** is affixed to a mail object **130** (as used in its broader sense to encompass the packaging that surrounds the content). It should be appreciated that mail ID data can be encoded/encrypted (e.g., using bar code data, digital data, etc.) to prevent fraudulent usage. It should further be appreciated that affixing the mail ID data **132** on the mail object **130** includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object **130** or printing/storing the mail ID data **132** on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object **130**. It should also be appreciated that the location of the mail ID data **132** on the mail object **130** in FIG. **1** is merely to exemplify how the invention operates, and is not intended to further limit the present invention. Thus, affixing the mail ID data **132** in some other location, such as over the sealing flap of an envelope, is within the spirit and scope of this invention.

At least a portion (i.e., a verifying portion) of the mail ID data **132** (either before or after the mail ID data is affixed) is stored in the mail ID device **110**, or more particular (as shown in FIG. **3**) in a memory **114** located within the mail ID device **110**. Specifically, the mail verification application **112** either receives or generates at least the verifying portion of the mail ID data **132**. The verifying portion is then stored in the memory **114**. In one embodiment of the present invention, the verifying portion of the mail ID data includes a identifiable code portion (e.g., an alpha code, a numeric code, and alpha-numeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.), and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail object **130**, which may further include a mail-to-address **134**, a return-mail-address **136**, and/or postage **138**, can then be manually delivered to a recipient. It should be appreciated that the mail ID data **132** can also be encoded (e.g., in a bar code, etc.) to include mail-to-address data, return-mail-address data, and/or postage data. In other words, for example, mail ID data could be encoded to include both coded data and postage-account data.

Once the recipient (or their designee) receives the mail object **130**, at least an authenticating portion of the mail ID data **132** is provided to the reception device **120**. The reception device **120**, which communicates with the mail ID device **110** over a wide area network **102**, transmits at least the authenticating portion of the mail identification data to the mail verification application **112** operating on the mail ID device **110**. The mail verification application **112** then compares the authenticating portion of the mail ID data with the verifying portion stored in memory **114**. If the received portion is authenticated, or corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device **120**.

In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (e.g., image data, audio data, etc.) indicating that the mail ID data has been authenticated. This would allow, for example, the reception device **120** to produce at least one authenticating image on a display and/or perform at least one authenticating sound on a speaker. In one embodiment of the present invention, at least a portion of the mail verification data includes securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating who is to receive the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page data, third party advertisements, etc.).

In another embodiment of the present invention, the mail ID device and/or the reception device further include an input device (e.g., **118**, **124**) adapted to receive at least a portion of the mail ID data. It should be appreciated that that the input devices depicted and discussed herein (e.g., **118**, **124**) include, but are not limited to, scanners (e.g., bar code scanners, etc.), keyboards, RFID readers, smart card readers, IC readers, and all other input devices generally known to those skilled in the art.

In another embodiment of the present invention, the mail ID device further includes an output device **116** adapted to affix (e.g., print, store, etc.) the mail ID data on the mail object. It should be appreciated that affixing the mail ID data on the mail object includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object or printing/storing the mail ID data on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object. It should further be appreciated that the output device depicted and described herein (e.g., **116**) includes, but is not limited to, printers, data storage device (e.g., device capable of storing data on ICs, smart cards, RFID tags, etc.), and all other output devices generally known to those skilled in the art.

In another embodiment of the present invention, as shown in FIG. **3**, the reception device **120** further includes a mail authenticating application **122** adapted to receive at least the authenticating portion of the mail ID data from the input device **124** and provide at least the authenticating portion of the mail ID data to the mail ID device. It should be appreciated that the mail authenticating application **122** may exist as a single application, or as multiple applications (locally and/or remotely stored) that operate together to perform the authenticating functions as described herein.

In one embodiment of the present invention, the mail ID data further includes software-booting data adapted to boot the mail authenticating application, an email application and/or a browser application. Either one of these applications could then be used to provide at least an authenticating portion of said mail ID data to said mail ID device, provide additional information to said mail ID device (or the sender of the mail object), and/or receive additional information from either the mail ID device, the sender of the mail object, or a third-party. In another embodiment, the mail verification data further includes software-booting data adapted to boot an email application and/or a browser application. Either one of these applications could then be used to provide additional information to the mail ID device and/or receive additional information from either the mail ID device, the sender of the mail object, or a third party.

In another embodiment of the invention, the reception device **120**, or more particularly the mail authenticating application **122** is adapted to provide a reply email to the mail ID device **130** or the sender of the mail object. This reply email may either be sent automatically, to acknowledge the reception of the mail ID data and/or mail verification data, or manually, to allow the recipient to communicate with the mail ID device and/or sender of the mail object. In another embodiment of the invention the mail verification application **112** is adapted to provide the mail verification data to the reception device **120** via an email.

In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient (as defined by this application) of the mail object **130**, thus interacting with the reception device **120** to receive mail verification data. If mail is authenticated (or approved in the case of screening), the mail object **130** is forwarded on to the actual intended recipient.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of the mail ID data. Specifically, in step **402** mail ID data is affixed to a mail object. At step **404**, a verifying portion of the mail ID data is stored in a memory device. The mail object is then delivered to its recipient (or designee) at step **406**. At step **408**, a reception device receives at least an authenticating portion of the mail ID data. The reception device then provides at least the authenticating portion to a mail ID device at step **410**. If the authenticating portion of the mail ID data corresponds to the verifying portion of the mail ID data, then mail verification data is provided to the reception device at step **412**. It should be appreciated that storing the verifying portion of the mail ID data before the mail ID data is affixed to the mail object is within the spirit and scope of the present invention.

Having thus described multiple embodiments of a system and method of providing mail verification data in response to receiving mail ID data, it should be apparent to those skilled in the art that certain advantages of the system have been achieved. It should also be appreciated that various modifications, adaptations, and alternative embodiments thereof may be made within the scope and spirit of the present invention. The invention is further defined by the following claims.

What is claimed is:

1. A method of verifying mail identification data, comprising:

affixing mail identification data to at least one mail object, said mail identification data comprising a single set of encoded data that includes at least a unique identifier, sender data, recipient data and shipping method data, wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object;

storing at least a verifying portion of said mail identification data;

receiving by a computer at least an authenticating portion of said mail identification data from at least one reception device via a network, wherein said authenticating portion of said mail identification data comprises at least said sender data and said shipping method data; and

providing by said computer mail verification data via said network when said authenticating portion of said mail identification data corresponds with said verifying portion of said mail identification data.

2. The method of claim **1**, wherein said step of affixing mail identification data further comprises affixing a bar code on said at least one mail object.

3. The method of claim **1**, wherein said step of affixing mail identification data further comprises printing said mail identification data at least indirectly on said at least one mail object.

4. The method of claim **1**, wherein said step of affixing mail identification data further comprises storing said mail identification data on a device attached to said at least one mail object.

5. The method of claim **1**, wherein said step of receiving at least an authenticating portion of said mail identification data further comprises receiving at least said authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion of said mail identification data further comprises at least said unique identifier.

6. The method of claim **5**, wherein said step of affixing mail identification data further comprises affixing at least a human readable version of said unique identifier on said at least one mail object.

7. The method of claim **5**, wherein said step of affixing mail identification data further comprises affixing at least a human readable version of recipient data on said at least one mail object.

8. The method of claim **5**, wherein said step of affixing mail identification data further comprises affixing at least a human readable version of said sender data on said at least one mail object.

9. The method of claim 1, wherein said step of receiving at least an authenticating portion of said mail identification data further comprises receiving at least said authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion of said mail identification data further comprises at least said recipient data.

10. The method of claim 1, wherein said step of receiving at least an authenticating portion of said mail identification data further comprises receiving at least said authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion of said mail identification data further comprises at least said recipient data and said unique identifier.

11. The method of claim 1, where said step of providing mail verification data further comprises providing said mail verification data to said at least one reception device.

12. The method of claim 1, wherein said step of providing mail verification data further comprises providing at least authenticating data to said at least one reception device.

13. The method of claim 1, wherein said step of providing mail verification data further comprises providing said mail verification data to a recipient of said at least one mail object.

14. The method of claim 13, wherein said step of providing mail verification data further comprises providing said mail verification data to said recipient of said at least one mail object via an email.

15. The method of claim 13, wherein said step of providing mail verification data further comprises providing at least said sender data to said recipient of said at least one mail object.

16. The method of claim 1, further comprising the step of sending a web page to a sender of said at least one mail object, said web page including data related to said at least one mail object.

17. The method of claim 1, further comprising the step of sending an email to a sender of said at least one mail object, said email including data related to said at least one mail object.

18. A method of verifying mail identification data, comprising:

receiving said mail identification data from a mail object, said mail identification data comprising a single set of encoded data that includes at least a unique identifier, recipient data, shipping method data and sender data, wherein said unique identifier consists of a numeric value that is assigned by a sender of said mail object;

providing by at least one computer at least said sender data and said shipping method data to a mail identification device over a network;

receiving by said at least one computer mail verification data from said mail identification device when said at least said sender data and said shipping method data are stored on said mail identification device, said mail verification data indicating, at least in part, that said at least one mail object was sent by an identifiable entity, and therefore traceable to a source; and

routing said at least one mail object to be delivered to a recipient if said mail verification data is received.

19. The method of claim 18, wherein said steps of providing at least said sender data and said shipping method data and receiving mail verification data further comprises providing at least said recipient data to said mail identification device over said network and receiving said mail verification data from said mail identification device if said sender data, said shipping method data and said at least said recipient data are stored on said mail identification device.

20. The method of claim 19, wherein said steps of providing at least said sender data, said shipping method data and said recipient data and receiving mail verification data further comprises providing at least said unique identifier to said mail identification device over said network and receiving said mail verification data from said mail identification device if said sender data, said unique identifier, said recipient data and said shipping method data are stored on said mail identification device.

21. The method of claim 18, wherein said steps of providing at least said sender data and said shipping method data and receiving mail verification data further comprises providing at least said unique identifier to said mail identification device over said network and receiving mail verification data from said mail identification device if said sender data, said shipping method data and said at least said unique identifier are stored on said mail identification device.

22. The method of claim 18, further comprising using said mail identification data to generate an email addressed to said mail identification device.

23. The method of claim 18, further comprising using said mail identification data to generate an email addressed to a sender of said mail object.

24. The method of claim 18, further comprising booting a mail authenticating application in response to receiving said mail identification data.

25. The method of claim 18, further comprising producing an authenticating image on a display after said mail verification data is received.

26. The method of claim 18, further comprising producing an authenticating-sound on at least one speaker after said mail verification data is received.

27. The method of claim 18, further comprising the step of sending a web page to a sender of said mail object, said web page including data related to said mail object.

28. The method of claim 27, wherein said steps of providing at least said sender data and said shipping method data and receiving mail verification data further comprises providing at least said unique identifier to said mail identification device over said network and receiving said mail verification data from said mail identification device if said sender data, said shipping method data and said at least said unique identifier are stored on said mail identification device.

29. The method of claim 28, wherein said steps of providing at least said sender data, said shipping method data and said unique identifier and receiving mail verification data further comprises providing at least said recipient data to said mail identification device over said network and receiving said mail verification data from said mail identification device if said sender data, said shipping method data, said unique identifier and said at least said recipient data are stored on said mail identification device.

30. The method of claim 18, further comprising the step of storing a shipping location of said mail object on said mail identification device.

31. The method of claim 18, further comprising the step of storing a shipping date of said mail object on said mail identification device.

32. The method of claim 18, further comprising the step of sending an email to a sender of said mail object, said email including data related to said mail object.

33. A mail verification system for authenticating at least one mail object, said at least one mail object being a physical object and including mail identification data, comprising:

at least one mail verification device adapted to communicate with at least one reception device via a network, said at least one mail verification device comprising:

a memory; and

a mail verification application adapted to:

store at least a verifying portion of mail identification data in said memory, said mail identification data comprising a single set of encoded data that includes at least a unique identifier, sender information, recipient information and shipping method information, wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object;

receive at least an authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion comprises at least said sender information and said shipping method information; and

provide mail verification data via said network if at least said authenticating portion of said mail identification data corresponds to said verifying portion of said mail identification data.

34. The mail verification system of claim **33**, wherein a portion of said mail verification application under said sender's control is further adapted to generate at least said verifying portion of said mail identification data.

35. The mail verification system of claim **34** further comprising an output device adapted to affix said mail identification data on said at least one mail object.

36. The mail verification system of claim **35**, wherein said output device is adapted to affix said mail identification data on said at least one mail object by printing said mail identification data on at least one label.

37. The mail verification system of claim **35**, wherein said output device is adapted to affix said mail identification data on said at least one mail object by storing said mail identification data on at least one tag.

38. The mail verification system of claim **33** further comprising an input device adapted to receive at least said verifying portion of said mail identification data.

39. The mail verification system of claim **33**, wherein said authenticating portion of said mail identification data further includes at least said unique identifier.

40. The mail verification system of claim **39**, wherein said authenticating portion of said mail identification data further includes at least said recipient information.

41. The mail verification system of claim **33**, wherein said mail identification data is encoded on said at least one mail object through a bar code.

42. The mail verification system of claim **33**, wherein a portion of said mail verification application under said sender's control is further adapted to generate at least said unique identifier.

43. The mail verification system of claim **33**, wherein said mail identification data further includes at least postage data.

44. The mail verification system of claim **33**, wherein said mail verification data includes at least authenticating data.

45. The mail verification system of claim **33**, wherein said mail verification data includes at least said sender information.

46. The mail verification system of claim **33**, wherein said mail identification data includes at least mail-object-content data.

47. The mail verification system of claim **33**, wherein said mail verification data includes at least securing data.

48. The mail verification system of claim **33**, wherein said mail verification application is further adapted to send an email in response to receiving said authenticating portion of said mail identification data.

49. The mail verification system of claim **33**, wherein said mail verification application is further adapted to send an email if said authenticating portion of said mail identification data corresponds to said verifying portion of said mail identification data.

50. The mail verification system of claim **33**, further comprising said at least one reception device.

51. The mail verification system of claim **50**, wherein said at least one reception device comprises an input device for receiving at least a portion of said mail identification data from said at least one mail object.

52. The mail verification system of claim **51**, wherein said at least one reception device further comprises a mail authenticating application adapted to:

receive said at least a portion of said mail identification data from said input device; and

provide at least said authenticating portion of said mail identification data to said at least one mail verification device.

53. The mail verification system of claim **52**, wherein said at least one reception device further includes a display, said mail authenticating application being further adapted to display at least one authenticating image on said display if said mail verification data is not received.

54. The mail verification system of claim **52**, wherein said at least one reception device further includes at least one speaker, said mail authenticating application being further adapted to produce at least one authenticating sound on said at least one speaker if said mail verification data is not received.

55. The mail verification system of claim **52**, wherein said mail authenticating application is further adapted to send an email in response to receiving said mail identification data.

56. The mail verification system of claim **52**, wherein said mail authenticating application is further adapted to send an email in response to receiving said mail verification data.

* * * * *

EXHIBIT 3

(12) **United States Patent**
Fitzsimmons

(10) **Patent No.: US 8,073,787 B2**
(45) **Date of Patent: *Dec. 6, 2011**

(54) **SYSTEM AND METHOD FOR MAIL VERIFICATION**

(76) Inventor: **Todd E. Fitzsimmons**, Long Beach, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 431 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/454,052**

(22) Filed: **May 11, 2009**

(65) **Prior Publication Data**

US 2009/0287344 A1 Nov. 19, 2009

Related U.S. Application Data

(63) Continuation of application No. 10/271,471, filed on Oct. 15, 2002, now Pat. No. 7,818,268.

(60) Provisional application No. 60/330,031, filed on Oct. 16, 2001.

(51) **Int. Cl.**

G06F 17/00	(2006.01)
G06F 21/00	(2006.01)
G06Q 10/00	(2006.01)
G06Q 20/00	(2006.01)
G07B 17/02	(2006.01)

(52) **U.S. Cl.** **705/401**; 705/1.1; 705/64; 705/402; 705/408; 713/186

(58) **Field of Classification Search** 705/1.1, 705/64, 401, 402, 408; 713/186

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,558,318	A	12/1985	Katz et al.
5,043,908	A	8/1991	Manduley et al.
5,684,705	A	11/1997	Herbert
5,963,927	A	10/1999	Herbert
5,984,366	A	11/1999	Priddy
6,260,029	B1	7/2001	Critelli
6,289,323	B1	9/2001	Gordon et al.
6,510,992	B2	1/2003	Wells et al.
6,539,360	B1	3/2003	Kadaba
6,810,408	B1	10/2004	Bates et al.
7,200,753	B1	4/2007	Shinzaki et al.
7,305,104	B2	12/2007	Carr et al.
2002/0029152	A1	3/2002	Lee et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP	09-099931	4/1997

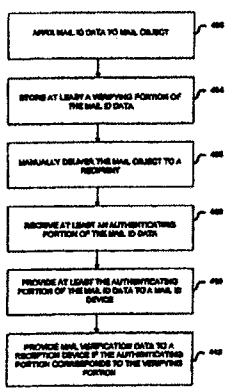
(Continued)

Primary Examiner — Fadey Jabr

(57) **ABSTRACT**

A system and method is provided for transmitting mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In one embodiment of the present invention, a mail verification application is adapted to store at least a verifying portion (e.g., an identifiable code portion, a shipping portion, a recipient portion, etc.) of mail ID data in memory. The mail ID data is then affixed to a mail object. The mail object is then manually delivered to a recipient. At least an authenticating portion of the mail ID data is then provided to a reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion of the mail ID data is authenticated, mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data, securing data, sender data, recipient data, mail-content data, downloadable-product data, sender-web-page data, and/or third-party-web-page data.

58 Claims, 3 Drawing Sheets



U.S. PATENT DOCUMENTS

2002/0083022	A1	6/2002	Algazi
2003/0004830	A1	1/2003	Frederick
2003/0101143	A1	5/2003	Montgomery et al.
2003/0101148	A1	5/2003	Montgomery et al.
2003/0102374	A1	6/2003	Wojdyla et al.
2003/0118191	A1	6/2003	Wang et al.
2003/0141358	A1	7/2003	Hudson et al.
2003/0177095	A1	9/2003	Zorab et al.

FOREIGN PATENT DOCUMENTS

JP	2001275159	10/2001
JP	2002284239	10/2002
WO	WO 96/03286	2/1996
WO	WO 96/13015	5/1996
WO	WO 01/35348	5/2001

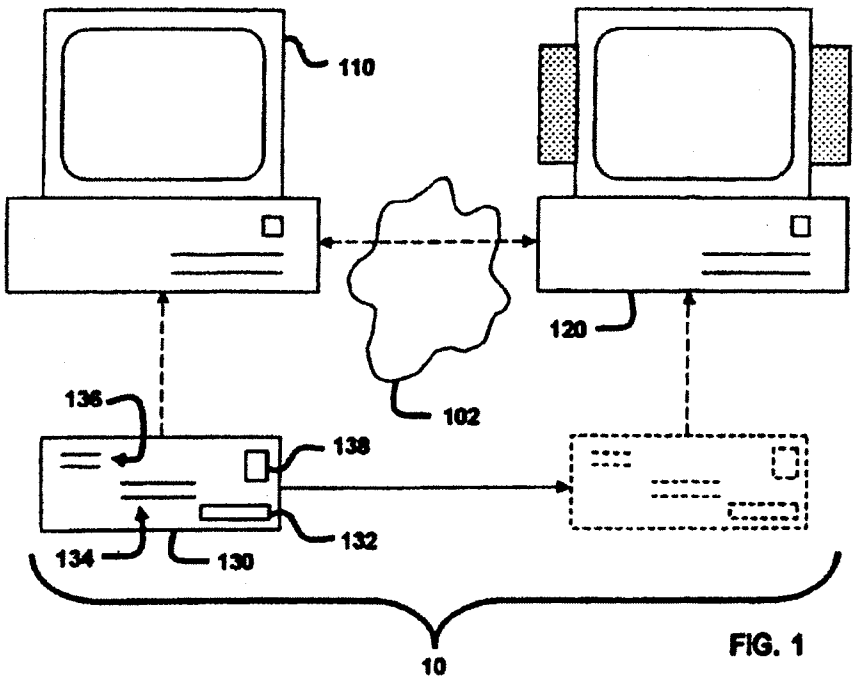


FIG. 1

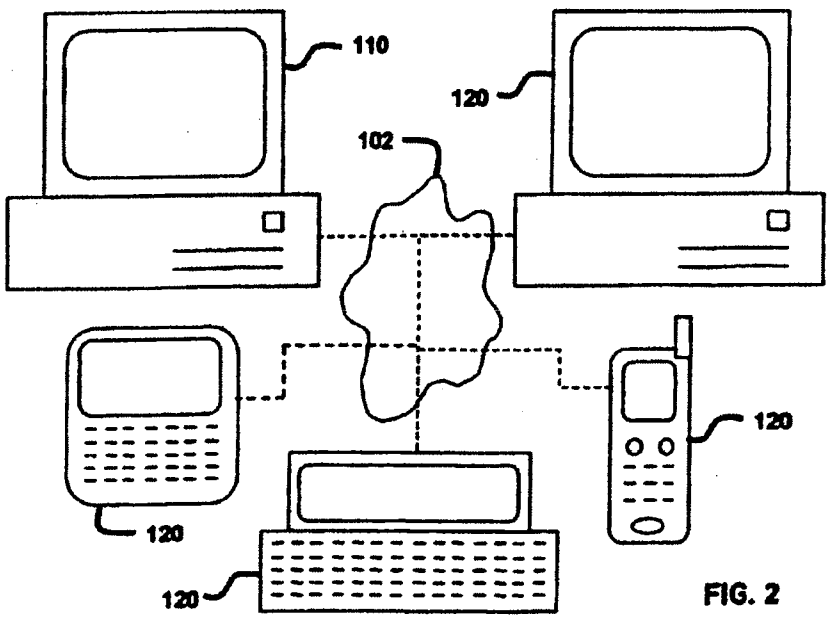


FIG. 2

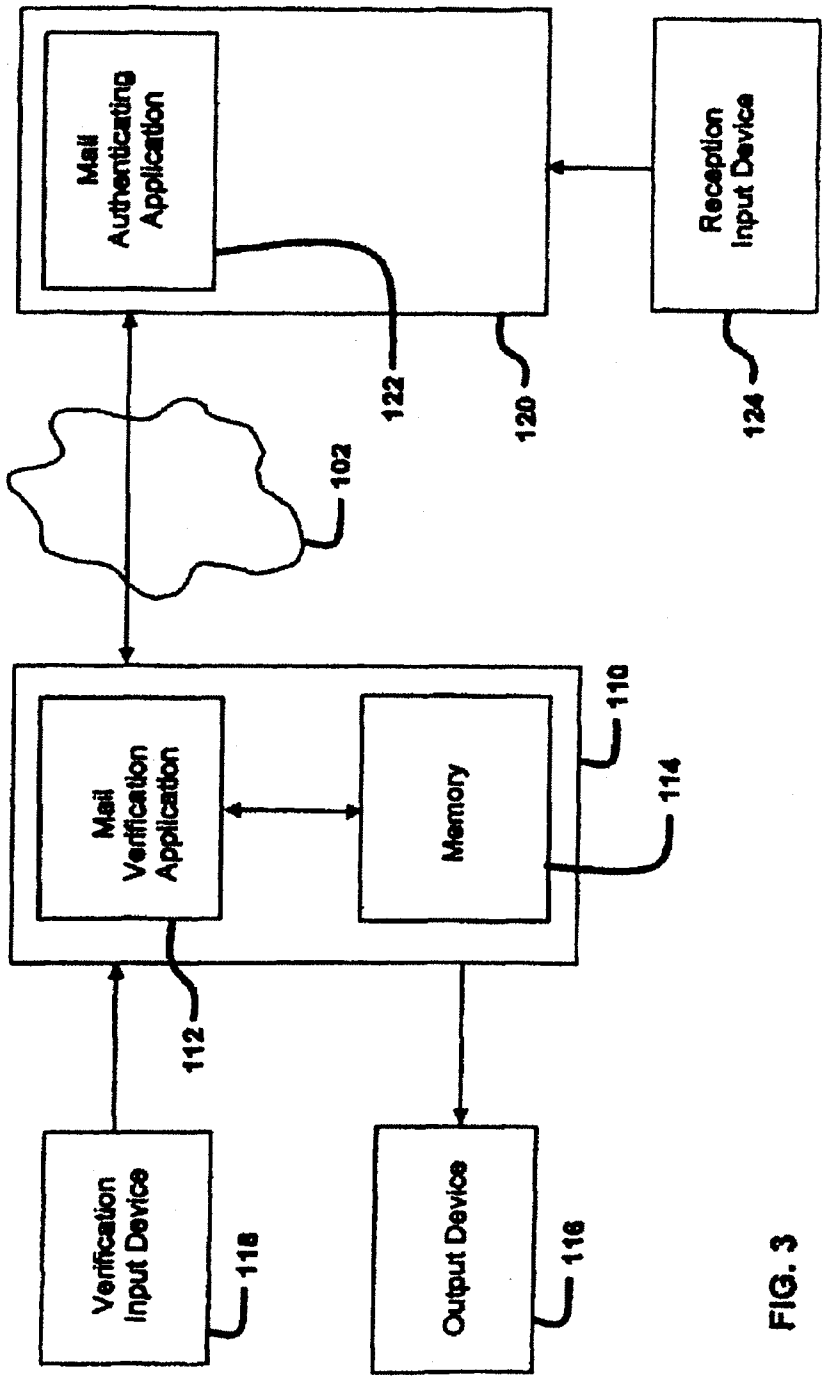

Mail Authenticating Application
Reception Input Device
122
120
124
102
Mail Verification Application
Memory
110
114
112
Verification Input Device
118
Output Device
118

FIG. 3

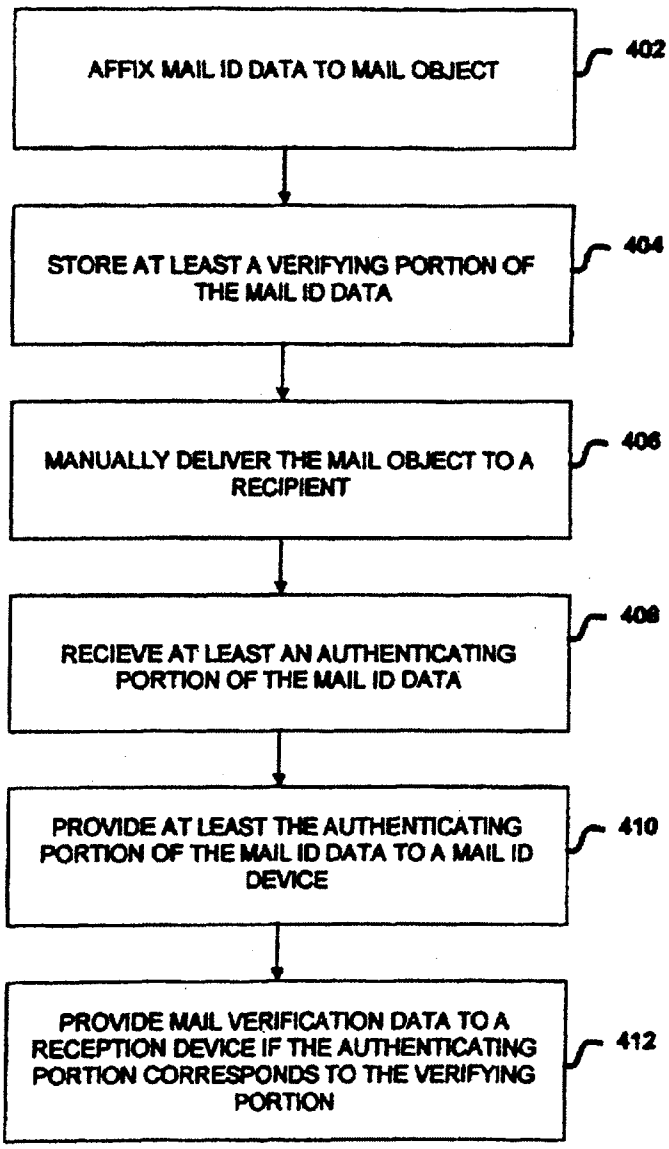

AFFIX MAIL ID DATA TO MAIL OBJECT
402
STORE AT LEAST A VERIFYING PORTION OF THE MAIL ID DATA
404
MANUALLY DELIVER THE MAIL OBJECT TO A RECIPIENT
406
RECIEVE AT LEAST AN AUTHENTICATING PORTION OF THE MAIL ID DATA
408
PROVIDE AT LEAST THE AUTHENTICATING PORTION OF THE MAIL ID DATA TO A MAIL ID DEVICE
410
PROVIDE MAIL VERIFICATION DATA TO A RECEPTION DEVICE IF THE AUTHENTICATING PORTION CORRESPONDS TO THE VERIFYING PORTION
412

FIG. 4

SYSTEM AND METHOD FOR MAIL VERIFICATION

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of U.S. patent application Ser. No. 10/271,471, filed Oct. 15, 2002, now U.S. Pat. No. 7,818,268 which claims the benefit pursuant to 35 U.S.C. §119(e) of U.S. Provisional Patent Application No. 60/330,031 filed Oct. 16, 2001, which applications are specifically incorporated herein, in their entirety, by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to mail verification, and more particularly to a system and method of authenticating at least one mail object by providing at least a portion of mail identification data over a wide area network, such as the Internet, in order to receive mail verification data.

2. Description of Related Art

Currently there are two ways to provided mail objects (e.g., letters, documents, packages, etc.) to an end user; that being electronically (e.g., email, etc.) and through traditional mail services (e.g., U.S. Postal Service, Federal Express, UPS, Courier, etc.). However, because certain mail objects cannot be delivered electronically (either because its impossible or impractical), they are delivered using traditional mail services.

There are several problems with delivering mail objects through traditional mail services. First, the mail object is typically secured inside packaging (e.g., envelops, boxes, etc.) before it is provided to the mail service. Thus, neither the mail service nor the recipient is aware of the contents of the package until such package is opened by the recipient. This creates a problem in that hazardous mail objects (i.e., Anthrax, explosives, etc.) are not detected until they are opened by the recipient, thus exposing the recipient to the hazardous material. It also creates a problem in that mail objects (in general) are not known until they are opened by the recipient, thus making it difficult for the recipient (or his designee) to properly screen, sort or avoid certain mail objects (e.g., offensive mail, annoying mail, etc).

Second, a manually delivered mail object is limited to a one-way production of a finite set of information and/or products. This becomes problematic when the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.). Finally, contents that can be delivered electronically (e.g., advertisements, software, etc.) are often included in mail objects that are delivered via traditional mail services. The drawback with this is that it increases the cost associated with producing and/or delivering the mail object and increase the size of the mail object. For at least these reasons, a need exists in the industry for a system and method of providing mail verification data in response to receiving mail ID data over a wide area network, such as the Internet.

SUMMARY OF THE INVENTION

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. Preferred embodiments of the present invention operate in accordance

with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. Specifically, the mail verification application is adapted to store at least a verifying portion of mail ID data in memory. In one embodiment of the present invention, the verifying portion of the mail ID data includes an identifiable code portion (e.g., an alpha code, a numeric code, an alphanumeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.) and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail ID data is then affixed to a mail object. The mail object, which may further include a mail-to-address, a return-mail-address, and/or postage, is then manually delivered to a recipient. In one embodiment of the present invention, the mail ID data further includes mail-to-address data, return-mail-address data, and/or postage data.

At least an authenticating portion of the mail ID data is then provided to the reception device. The reception device, which communicates with the mail ID device over a wide area network, transmits at least the authenticating portion of the mail ID data to the mail verification application operating on the mail ID device. The mail verification application then compares the authenticating portion of the mail ID data with the verifying portion stored in memory. If the authenticating portion corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device. In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (indicating that the mail ID data has been authenticated), securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating the intended recipient of the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page information, third party advertisements, etc).

In one embodiment of the present invention, the mail ID device further includes an input device adapted to provide at least a verifying portion of the mail ID data to the mail verification application and/or an output device adapted to affix the mail ID data on the mail object. In another embodiment of the present invention, the reception device includes an input device for receiving at least an authenticating portion of the mail ID data from the mail object and/or a mail authenticating application adapted to receive at least the authenticating portion of the mail ID data from the input device and provide at least the authenticating portion of the mail ID data to the mail ID device. In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient of the mail object, thus interacting with the reception device to receive mail verification data.

A more complete understanding of the system and method for providing mail verification data in response to receiving at least a portion of mail ID data will be afforded to those skilled in the art, as well as a realization of additional advantages and objects thereof, by a consideration of the following detailed description of the preferred embodiment. Reference will be made to the appended sheets of drawings which will first be described briefly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates one embodiment of the mail verification system.

FIG. **2** illustrates a mail ID device communicating with a plurality of reception devices over a wide area network, such as the Internet.

FIG. **3** illustrates one embodiment of the mail ID device and the reception device depicted in FIG. **1**.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of mail ID data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system and method for providing mail verification data over a wide area network, such as the Internet, in response to receiving and authenticating at least a portion of mail identification (ID) data. In the detailed description that follows, like element numerals are used to describe like elements illustrated in one or more figures.

Preferred embodiments of the present invention operate in accordance with at least one reception device, a mail identification (ID) device, a memory, and a mail verification application adapted to communicate with the reception device over a wide area network, such as the Internet. FIG. **1** illustrates one embodiment of the mail verification system **10**, which includes a mail ID device **110** and a reception device **120** communicating through a wide area network **102**, such as the Internet. It should be appreciate, as depicted in FIG. **2**, that the reception device(s) **120** includes, but is not limited to, personal computers, set top boxes, personal digital assistances (PDAs), mobile phones, land-line phones, televisions, bar code readers, and all other physically and wirelessly connected reception devices generally known to those skilled in the art. It should further be appreciated that the number of reception devices **120** depicted in FIGS. **1** and **2** are merely to illustrate how the present invention operates, and are not intended to further limit the present invention.

As shown in FIG. **3**, the mail ID device **110** further includes a mail verification application **112** and a memory **114**. The mail verification application **112** is adapted to store at least a portion (i.e., a verifying portion) of mail ID data in the memory **114**, receive at least a portion (i.e., an authenticating portion) of mail ID data from the reception device **120**, and provide mail verification data if the portion of the mail ID data received from the reception device **120** is authenticated. It should be appreciated that the mail verification application **112** may further be adapted to generate the mail ID data and provide it to an external device (e.g., a printer, etc.) or receive at least a verifying portion of the mail ID data from an external device (e.g., a scanner, etc.). It should also be appreciated that the mail verification application **112** may exist as a single application, or as multiple applications (locally and/or remotely stored) that operate together to perform the verification functions as described herein. It should further be appreciated that the location of the memory device **114** depicted in FIG. **3** is not intended to further limit the present invention. Thus, a memory device that is, for example, external to the mail ID device **110** is within the spirit and scope of the present invention.

Referring back to FIG. **1**, where the dashed arrows indicate data transactions and the solid arrow indicates physical movement, mail ID data **132** is affixed to a mail object **130** (as used in its broader sense to encompass the packaging that surrounds the content). It should be appreciated that mail ID data can be encoded/encrypted (e.g., using bar code data, digital data, etc.) to prevent fraudulent usage. It should further be appreciated that affixing the mail ID data **132** on the mail object **130** includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object **130** or printing/storing the mail ID data **132** on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object **130**. It should also be appreciated that the location of the mail ID data **132** on the mail object **130** in FIG. **1** is merely to exemplify how the invention operates, and is not intended to further limit the present invention. Thus, affixing the mail ID data **132** in some other location, such as over the sealing flap of an envelope, is within the spirit and scope of this invention.

At least a portion (i.e., a verifying portion) of the mail ID data **132** (either before or after the mail ID data is affixed) is stored in the mail ID device **110**, or more particular (as shown in FIG. **3**) in a memory **114** located within the mail ID device **110**. Specifically, the mail verification application **112** either receives or generates at least the verifying portion of the mail ID data **132**. The verifying portion is then stored in the memory **114**. In one embodiment of the present invention, the verifying portion of the mail ID data includes a identifiable code portion (e.g., an alpha code, a numeric code, and alpha-numeric code, a symbolic code, a digital code, etc.), a shipping portion (e.g., ship date, shipping location, shipping method, etc.), and/or a recipient portion (e.g., the recipients name, address, email address, IP address, account number, social security number, etc.). The mail object **130**, which may further include a mail-to-address **134**, a return-mail-address **136**, and/or postage **138**, can then be manually delivered to a recipient. It should be appreciated that the mail ID data **132** can also be encoded (e.g., in a bar code, etc.) to include mail-to-address data, return-mail-address data, and/or postage data. In other words, for example, mail ID data could be encoded to include both coded data and postage-account data.

Once the recipient (or their designee) receives the mail object **130**, at least an authenticating portion of the mail ID data **132** is provided to the reception device **120**. The reception device **120**, which communicates with the mail ID device **110** over a wide area network **102**, transmits at least the authenticating portion of the mail identification data to the mail verification application **112** operating on the mail ID device **110**. The mail verification application **112** then compares the authenticating portion of the mail ID data with the verifying portion stored in memory **114**. If the received portion is authenticated, or corresponds to the verifying portion (e.g., matches, is reasonably related, etc.), then mail verification data is sent to the reception device **120**.

In one embodiment of the present invention, at least a portion of the mail verification data includes authenticating data (e.g., image data, audio data, etc.) indicating that the mail ID data has been authenticated. This would allow, for example, the reception device **120** to produce at least one authenticating image on a display and/or perform at least one authenticating sound on a speaker. In another embodiment of the present invention at least a portion of the mail verification data includes securing data (indicating who secured the mail object), sender data (indicating who sent the mail object), recipient data (indicating who is to receive the mail object) and/or additional data (e.g., the contents of the mail object, downloadable product data, sender web-page data, third party advertisements, etc).

In another embodiment of the present invention, the mail ID device and/or the reception device further include an input

device (e.g., **118**, **124**) adapted to receive at least a portion of the mail ID data. It should be appreciated that that the input devices depicted and discussed herein (e.g., **118**, **124**) include, but are not limited to, scanners (e.g., bar code scanners, etc.), keyboards, RFID readers, smart card readers, IC readers, and all other input devices generally known to those skilled in the art.

In another embodiment of the present invention, the mail ID device further includes an output device **116** adapted to affix (e.g., print, store, etc.) the mail ID data on the mail object. It should be appreciated that affixing the mail ID data on the mail object includes, but is not limited to, printing or attaching mail ID data directly on the outer surface of the mail object or printing/storing the mail ID data on labels, ICs, smart cards, RFID tags, or any other data storage devices (or materials) generally known to those skilled in the art, and attaching them to the outer surface of the mail object. It should further be appreciated that the output device depicted and described herein (e.g., **116**) includes, but is not limited to, printers, data storage device (e.g., device capable of storing data on ICs, smart cards, RFID tags, etc.), and all other output devices generally known to those skilled in the art.

In another embodiment of the present invention, as shown in FIG. **3**, the reception device **120** further includes a mail authenticating application **122** adapted to receive at least the authenticating portion of the mail ID data from the input device **124** and provide at least the authenticating portion of the mail ID data to the mail ID device. It should be appreciated that the mail authenticating application **122** may exist as a single application, or as multiple applications (locally and/or remotely stored) that operate together to perform the authenticating functions as described herein.

In one embodiment of the present invention, the mail ID data further includes software-booting data adapted to boot the mail authenticating application, an email application and/or a browser application. Either one of these applications could then be used to provide at least an authenticating portion of said mail ID data to said mail ID device, provide additional information to said mail ID device (or the sender of the mail object), and/or receive additional information from either the mail ID device, the sender of the mail object, or a third-party. In another embodiment, the mail verification data further includes software-booting data adapted to boot an email application and/or a browser application. Either one of these applications could then be used to provide additional information to the mail ID device and/or receive additional information from either the mail ID device, the sender of the mail object, or a third party.

In another embodiment of the invention, the reception device **120**, or more particularly the mail authenticating application **122** is adapted to provide a reply email to the mail ID device **130** or the sender of the mail object. This reply email may either be sent automatically, to acknowledge the reception of the mail ID data and/or mail verification data, or manually, to allow the recipient to communicate with the mail ID device and/or sender of the mail object. In another embodiment of the invention the mail verification application **112** is adapted to provide the mail verification data to the reception device **120** via an email.

In another embodiment of the present invention, the U.S. Postal Service (or an interim authenticating or screening entity) is the recipient (as defined by this application) of the mail object **130**, thus interacting with the reception device **120** to receive mail verification data. If mail is authenticated (or approved in the case of screening), the mail object **130** is forwarded on to the actual intended recipient.

FIG. **4** is a flow chart illustrating one method of providing mail verification data in response to receiving at least a portion of the mail ID data. Specifically, in step **402** mail ID data is affixed to a mail object. At step **404**, a verifying portion of the mail ID data is stored in a memory device. The mail object is then delivered to its recipient (or designee) at step **406**. At step **408**, a reception device receives at least an authenticating portion of the mail ID data. The reception device then provides at least the authenticating portion to a mail ID device at step **410**. If the authenticating portion of the mail ID data corresponds to the verifying portion of the mail ID data, then mail verification data is provided to the reception device at step **412**. It should be appreciated that storing the verifying portion of the mail ID data before the mail ID data is affixed to the mail object is within the spirit and scope of the present invention.

Having thus described multiple embodiments of a system and method of providing mail verification data in response to receiving mail ID data, it should be apparent to those skilled in the art that certain advantages of the system have been achieved. It should also be appreciated that various modifications, adaptations, and alternative embodiments thereof may be made within the scope and spirit of the present invention. The invention is further defined by the following claims.

What is claimed is:

1. A system for authenticating a mail object, said mail object being provided to a mail carrier and including mail identification data affixed on said mail object in a single barcode, comprising:

a first computer configured to communicate at least a first portion of said mail identification data over a network, said mail identification data including a shipping portion, a recipient portion, a sender portion, and an identifier portion, wherein said shipping portion includes shipping method data, said recipient portion includes an address of a recipient of said mail object, and said identifier portion includes a unique identifier that consists of a numeric value assigned by a sender of said mail object;

a database; and

a second computer comprising a verification application, said second computer being configured to receive at least said first portion of said mail identification data from said first computer via said network, said first portion of said mail identification data consisting of said shipping portion, said sender portion and said identifier portion;

wherein said verification application is in communication with said database and configured to authenticate said first portion of said mail identification data by determining whether said first portion of said mail identification data is stored in said database and providing verifying data to said first computer via said network, said verifying data indicating whether said first portion of said mail identification data is stored in said database, wherein at least a portion of said first portion can be used by said mail carrier to identify said sender of said mail object.

2. The system of claim **1**, wherein said first computer is further configured to generate said unique identifier.

3. The system of claim **1**, wherein said first computer further comprises an output device for affixing said barcode onto said mail object.

4. The system of claim **3**, wherein said first computer is further configured to encode said mail identification data into said barcode prior to said barcode being affixed to said mail object.

5. The system of claim 4, wherein said first computer is further configured to encrypt said mail identification data before it is encoded into said barcode.

6. The system of claim 1, wherein said sender portion includes data that is assigned by said mail carrier and can be used by said mail carrier to identify said sender of said mail object.

7. The system of claim 6, wherein said verifying data further includes postage data pertaining to said mail object.

8. The system of claim 7, wherein said verification application is further configured to determine whether said first portion of said mail identification data is stored in said database and to provide said verifying data to said first computer before said mail object is accepted by said mail carrier.

9. The system of claim 6, wherein said first computer is further configured to communicate said first portion of said mail identification data to said second computer before said mail object is provided to said mail carrier.

10. The system of claim 1, wherein said verifying data further includes postage data pertaining to said mail object.

11. The system of claim 10, wherein said verification application is further configured to generate an email concerning said verifying data and provide said email to said first computer.

12. The system of claim 1, wherein said verification application is further configured to determine whether said first portion of said mail identification data is stored in said database and to provide said verifying data to said first computer before said mail object is accepted by said mail carrier.

13. The system of claim 1, wherein said first computer is further configured to communicate second mail identification data to said second computer, said second mail identification data being affixed in a single barcode to a second mail object provided to said mail carrier, wherein said second mail identification data includes sender data and a second unique identifier assigned by said sender, and said verification application is further configured to determine whether said second mail identification data is stored in said database, wherein said verifying data further indicates whether said second mail identification data is stored in said database.

14. The system of claim 13, wherein said verifying data further includes content data pertaining to said second mail object.

15. The system of claim 13, wherein said verifying data further includes postage data pertaining to said second mail object.

16. The system of claim 14, wherein said second mail identification data further includes destination data and shipping method data.

17. A method for authenticating a mail object, said mail object including mail identification data affixed on said mail object as a single barcode, comprising:

communicating by at least one computer at least a first portion of said mail identification data over a network, said mail identification data includes a shipping portion, a recipient portion, a sender portion, and an identifier portion, wherein said shipping portion includes shipping method data, said recipient portion includes destination data of said mail object, and said identifier portion consists of a numeric value assigned by a sender of said mail object; and

receiving by a second computer at least said first portion of said mail identification data, said first portion of said mail identification data consisting of said shipping portion, said sender portion and said identifier portion;

determining by said second computer whether said first portion of said mail identification data is stored in a database in communication with said second computer; and

generating at least one electronic file in response to said step of determining whether said first portion is stored on said database, said at least one electronic file comprising verification data and postage data, said verification data providing whether said first portion of said mail identification data is stored in said database;

wherein said at least one electronic file is accessible to said at least one computer and at least a portion of said first portion of said mail identification data can be used by a mail carrier to identify said sender.

18. The method of claim 17, further comprising:

encoding said mail identification data in said single barcode;

affixing by an output device said single barcode on said mail object; and

providing said mail object to said mail carrier.

19. The method of claim 18, further comprising using an algorithm to digitally code said mail identification data prior to encoding said mail identification data in said single barcode.

20. The method of claim 18, wherein said sender portion includes sender data that is assigned by said mail carrier, wherein said sender data can be used by said mail carrier to identify said sender of said mail object.

21. The method of claim 20, wherein said steps of determining whether said first portion of said mail identification data is stored in said database and generating said at least one electronic file are performed before said mail object is accepted by said mail carrier.

22. The method of claim 20, further comprising:

communicating by said at least one computer second mail identification data to said second computer, said second mail identification data being affixed as a single barcode on a second object provided to said mail carrier and including at least said sender data and an identifier assigned by said sender;

determining by said second computer whether said second mail identification data is stored in said database, wherein said verification data further provides whether said second mail identification data is stored in said database.

23. The method of claim 22, wherein said verification data further includes content data pertaining to said second object.

24. The method of claim 23, further comprising scanning said single barcode on said second object to acquire said second mail identification data, determining whether said second mail identification data is stored in said database, and providing data to said at least one computer if said second mail identification data is stored in said database, said data indicating that said second object has been received by said mail carrier.

25. The method of claim 22, further comprising scanning said single barcode on said second object to acquire said second mail identification data, determining whether said second mail identification data is stored in said database, and providing content data pertaining to said second object over said network if said second mail identification data is stored in said database.

26. The method of claim 18, further comprising providing said at least one electronic file to said at least one computer via said network, wherein said steps of determining whether said first portion of said mail identification data is stored in

said database and providing said verifying data to said at least one computer are performed before said mail object is accepted by said mail carrier.

27. The method of claim **18**, wherein said step of communicating at least said first portion of said mail identification data over said network is performed before said step of providing said mail object to said mail carrier.

28. The method of claim **17**, wherein said postage data pertains to at least said mail object.

29. The method of claim **17**, further comprising generating an email concerning said verifying data, and addressing said email to said sender of said mail object.

30. A method for authenticating a mail object that includes mail identification data, said mail identification data being encoded into a single barcode, which is then affixed onto said mail object, comprising:

communicating by at least one sender computer at least a first portion of said mail identification data over a network, said mail identification data including a shipping portion including at least shipping method data, a recipient portion including destination data for said mail object, a sender portion, and an identifier portion including at least a numeric value assigned by a sender of said mail object, and said first portion of said mail identification data consisting of said shipping portion, said sender portion and said identifier portion;

receiving by said at least one sender computer verifying data from a second computer via a network, wherein said verifying data verifies the authenticity of said first portion of said mail identification data by stating whether said first portion corresponds to data that is stored on a database in communication with said second computer;

providing said mail object to a mail carrier, wherein at least a portion of said first portion can be used by said mail carrier to identify said sender of said mail object.

31. The method of claim **30**, further comprising using an algorithm to encrypt said mail identification data prior to encoding said mail identification date in a single barcode.

32. The method of claim **30**, wherein said sender portion includes data that is assigned by said mail carrier and can be used to identify a sender of said mail object.

33. The method of claim **30**, wherein said step of communicating at least said first portion of said mail identification data over said network is performed before said step of providing said mail object to said mail carrier, and said verifying data states whether said first portion of said mail identification data, as communicated by said at least one sender computer, corresponds to data that is stored on said database.

34. The method of claim **30**, wherein said step of receiving verifying data is performed before said mail object is routed by said mail carrier through a mail stream to a recipient of said mail object.

35. The method of claim **30**, further comprising:

communicating by said at least one sender computer second mail identification data to said second computer, said second mail identification data being affixed as a single barcode on a second object provided to said mail carrier and including at least sender data and an identifier assigned by said sender;

wherein said verifying data further states whether said second mail identification data corresponds to data that is stored in said database.

36. The method of claim **35**, wherein said verifying data further includes data on a content of said second object.

37. The method of claim **35**, wherein said verifying data further includes postage data pertaining to said second object.

38. The method of claim **36**, wherein said verifying data further includes postage data pertaining to said second object.

39. The method of claim **36**, further comprising:

scanning said single barcode on said second object to retrieve said second mail identification data;

providing data to said at least one sender computer if said second mail identification data is stored in said database, said data indicating that said second object has been received by said mail carrier.

40. The method of claim **35**, further comprising:

scanning said single barcode on said second object to retrieve said second mail identification data;

providing to said at least one sender computer data on a content of said second object if said second mail identification data corresponds to data that is stored on said database.

41. A method for providing electronic data concerning a mail object having mail identification data encoded into a single barcode and affixed to said mail object, comprising:

receiving by at least a first computer at least a first portion of said mail identification data from said mail object, said mail identification data including a shipping portion including at least shipping method data, a recipient portion including destination data for said mail object, a sender portion, and an identifier portion comprising a numeric value, and said first portion of said mail identification data consisting of said shipping portion, said sender portion, and said identifier portion;

determining by said at least said first computer whether said first portion of said mail identification data is stored in a database in communication with said at least said first computer;

providing by said at least said first computer said electronic data to at least a second computer via a network, wherein said electronic data is generated when said first portion of said mail identification data matches data that is stored in said database.

42. The method of claim **41**, further comprising the step of providing by said at least said second computer at least a portion of said electronic data to a third computer via said network.

43. The method of claim **42**, wherein said step of providing by said at least said second computer at least a portion of said electronic data to a third computer further comprises providing said at least a portion of said electronic data to said third computer via an email.

44. The method of claim **42**, wherein said step of providing by said at least said second computer at least a portion of said electronic data to a third computer further comprises providing said at least a portion of said electronic data to said third computer via a web page.

45. The method of claim **44**, further comprising the step of generating by said at least said second computer said numeric value.

46. The method of claim **44**, further comprising the step of providing by said at least said second computer an email concerning said mail object to said third computer via said network.

47. The method of claim **46**, wherein said email is provided automatically in response to the reception of the mail object by the United States Postal Service.

48. The method of claim **42**, further comprising the step of providing by said at least said second computer additional information concerning said mail object to said third computer via said network, said additional information being at least one of information on a recipient of said mail object,

information on a sender of said mail object, and postage information on at least said mail object.

49. The method of claim **48**, wherein said additional information further indicates whether said mail object has been received by the United States Postal Service.

50. A system for providing electronic data concerning a mail object having mail identification data encoded into a single barcode and affixed to said mail object, comprising:

a scanner configured to scan at least a first portion of said mail identification data from said mail object, said mail identification data including a shipping portion including at least shipping method data, a recipient portion including destination data for said mail object, a mailer portion, and an identifier portion comprising a numeric value assigned by a mailer of said mail object, and said first portion of said mail identification data consisting of said shipping portion, said mailer portion, and said identifier portion;

a database for storing data on said mail object;

at least a first computer in communication with said scanner and said database; and

at least one application running on said at least said first computer and configured to (i) receive at least a first portion of said mail identification data from said scanner, (ii) determine whether said first portion of said mail identification data is stored in said database, and (iii) provide said electronic data to at least a second computer via a network, wherein said electronic data is generated when said first portion of said mail identification data matches said data that is stored in said database.

51. The method of claim **50**, further comprising at least said second computer having at least one other application configured to provide at least a portion of said electronic data to a third computer via said network and via at least one of an email and a web page.

52. The system of claim **51**, wherein said at least one other application is further configured to generate said numeric value.

53. The system of claim **51**, wherein said at least one other application is further configured to provide an email concerning said mail object to said third computer via said network.

54. The system of claim **51**, wherein said at least one other application is further configured to provide additional information concerning said mail object to said third computer via said network, said additional information being at least one of information on a recipient of said mail object, information on a sender of said mail object, and information on postage of at least said mail object.

55. The system of claim **53**, wherein said email is provided automatically in response to said mail object being received by a recipient of said mail object.

56. The system of claim **53**, wherein said email is provided automatically in response to said mail object being received by the United States Postal Service.

57. The system of claim **54**, wherein said additional information further indicates whether said mail object has been received by a recipient of said mail object.

58. The system of claim **54**, wherein said additional information indicates whether said mail object has been received by the United States Postal Service.

* * * * *