

No.

IN THE
Supreme Court of the United States

SECURED MAIL SOLUTIONS LLC,
Petitioner,

v.

UNIVERSAL WILDE, INC.,
Respondent.

**On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Federal Circuit**

PETITION FOR A WRIT OF CERTIORARI

TODD E. FITZSIMMONS*
FITZSIMMONS IP LAW
P.O. Box 199
Gardena, CA 90248
(213) 500-1178

Counsel for Petitioner

January 16, 2018

* Counsel of Record

QUESTIONS PRESENTED

In *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347 (2014), the Court set forth its two-part test for determining whether an invention is patent-eligible under 35 U.S.C. § 101: (1) whether the patent claims are directed to a patent ineligible concept, such as laws of nature, natural phenomena, or abstract ideas, and (2) if so, whether the elements of the claim contain an “inventive concept” that transforms the ineligible concept into an invention that is patent-eligible.

The questions presented are:

1) In determining patent-eligible subject matter within the meaning of 35 U.S.C. § 101, when a claim has been found to be directed to an abstract idea (the first part of *Alice*), should courts consider whether the claim substantially preempts the identified abstract idea in determining whether the claim includes an “inventive concept” (the second part of *Alice*)?

2) Because “[a]t some level, ‘all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas’” (*id.* at 2354), does the second part of *Alice* function as a safeguard, preventing claims that do not substantially preempt the identified abstract idea from falling victim to a misapplication of this exclusionary principle, which is often due to findings on inventiveness that are more properly addressed under 35 U.S.C. §§ 102 and 103.

PARTIES TO THE PROCEEDING

All parties to the proceedings are identified in the caption.

RULE 29.6 STATEMENT

Petitioner Secured Mail Solutions LLC has no parent corporations and no publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

	Page
QUESTIONS PRESENTED	i
PARTIES TO THE PROCEEDING.....	ii
RULE 29.6 STATEMENT.....	ii
TABLE OF CONTENTS	iii
TABLE OF AUTHORITIES	v
PETITION FOR A WRIT OF CERTIORARI	1
OPINIONS BELOW.....	1
JURISDICTION.....	1
STATUTORY PROVISIONS INVOLVED	1
INTRODUCTION	1
STATEMENT OF THE CASE.....	5
I. THE INVENTION.....	5
II.PROCEEDINGS BELOW	9
A. LOWER COURT PROCEEDINGS.....	9
B. FEDERAL CIRCUIT DECISION.....	13
REASONS FOR GRANTING THE PETITION	14
I. CERTIORARI IS NEEDED TO ENSURE THAT THE UNDERLYING PRINCIPLE OF PREEMPTION IS CONSIDERED WHEN DETERMINING WHETHER A CLAIM INCLUDES AN INVENTIVE CONCEPT.....	14

II. CERTIORARI IS NEEDED TO RE- SOLVE CONFLICTING APPROACH- ES TAKEN BY LOWER COURTS IN DETERMINING WHETHER A CLAIM INCLUDES AN INVENTIVE CON- CEPT.....	18
CONCLUSION.....	21

APPENDIX TABLE OF CONTENTS

ORDER OF THE FEDERAL CIRCUIT AF- FIRMING ORDER GRANTING DE- FENDANT'S MOTION TO DISMISS (October 16, 2017)	1a
ORDER GRANTING DEFENDANT'S MO- TION TO DISMISS (February 16, 2016)....	15a
FINAL ORDER ON CLAIM CONSTRUCTION (April 8, 2014).....	54a
SUPPLEMENTAL STATEMENT RE: PETI- TION TO MAKE SPECIAL (September 2, 2003).....	84A
DECISION ON PETITON TO MAKE SPE- CIAL (COUNTER TERRORISM) (October 8, 2003)	87a
RECORD OF ORAL HEARING UNITED STATES PATENT AND TRADEMARK OFFICE (June 8, 2010)	89a
PATENT NO. 7,818,268 B2 (October 19, 2010) ..	110a
PATENT NO. 9,105,002 B2 (August 11, 2015)...	120a

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Alice Corp. Pty. Ltd. v. CLS Bank Int'l</i> 134 S. Ct. 2347 (2014).....	2, 4, 10-13, 15-17
<i>Bilski v. Kappos</i> , 130 S. Ct. 3218 (2010).....	15
<i>California Inst. of Tech v. Hughes</i> <i>Commc'ns Inc.</i> , 59 F. Supp. 974 (C.D. Cal. 2014).....	14, 15
<i>Diamond v. Diehr</i> , 450 U.S. 63 (1972).....	14, 15
<i>Gottschalk v. Benson</i> , 409 U.S. 63 (1972).....	14, 15
<i>Mayo Collaborative Services v.</i> <i>Prometheus Laboratories, Inc.</i> , 132 S. Ct. 1289 (2012).....	15
<i>MySpace, Inc. v. GraphOn Corp.</i> , 672 F.3d 1250 (Fed Cir. 2012).....	2, 19, 20
<i>Parker v. Flook</i> , 437 U.S. 584 (1978).....	15, 19

STATUTES

28 U.S.C. § 1254(1).....	1
35 U.S.C. § 101	1, 2, 4, 10, 14, 15, 19, 20
35 U.S.C. § 102	4, 19, 20
35 U.S.C. § 103	4, 19, 20
35 U.S.C. § 112	19, 20

PETITION FOR A WRIT OF CERTIORARI

Petitioner Secured Mail Solutions LLC (“Petitioner”) respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Federal Circuit.

OPINIONS BELOW

The Federal Circuit’s Opinion affirming the Central District of California’s Order Granting Defendant’s Motion to Dismiss is unreported, but is reproduced in the appendix to this petition at 1a-14a. No petitions for rehearing were filed. The Central District of California’s Order Granting Defendant’s Motion to Dismiss is reported at 169 F. Supp. 1039, and is reproduced in the appendix to this petition at 15a-53a. The Central District of California’s Final Order on Claim Construction is unreported, but is reproduced in the appendix to this petition at 54a-83a.

JURISDICTION

The Federal Circuit issued its Order affirming the District Court’s Order Granting Defendant’s Motion to Dismiss on October 16, 2017. *See* Appendix at 1a-14a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

STATUTORY PROVISIONS INVOLVED

Section 101 of the Patent Act provides: “Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.” 35 U.S.C. § 101.

INTRODUCTION

In *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347 (2014), the Court reaffirmed its two-part test for determining whether an invention is patent-eligible under 35 U.S.C. § 101. The first part of the *Alice* test, determining whether the claim is directed to a patent ineligible concept, such as an abstract idea, can be difficult for courts to apply since “[a]t some level, ‘all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.’” *Id.* at 2354. Because of this, the second part of the *Alice* test, determining whether the claim contains an “inventive concept” sufficient to transform the claimed abstract idea into a patent-eligible application, is often the only part of *Alice* that prevents this exclusionary principle from “swallow[ing] all of patent law”—a concern expressed by the Court. *Id.*

However, Courts admittedly struggle in applying the second part of the *Alice* test. In this case, the district court stated that “[p]inning down the exclusion for ‘abstract ideas’ can be particularly challenging.” See Appendix to this Petition (“App”) at 27a-28a. While the district court attempted to apply the *Alice* test, it characterized Section 101 jurisprudence as a “murky morass,” and noted that “[courts] spend page after page revisiting our cases and those of the Supreme Court, and still we continue to disagree vigorously over what is or is not patentable subject matter.” *Id.* (quoting *MySpace, Inc. v. GraphOn Corp.*, 672 F.3d 1250, 1259 (Fed. Cir. 2012)).

This confusion can be seen in the district court’s analysis of whether the patents-in-suit, *i.e.*, patents

owned by Plaintiff Secured Mail Solutions LLC (“SMS”), claimed patent-eligible subject matter. For example, when SMS argued that the claimed inventions solved a specific problem in mailing technology, and cited the specification and the prosecution history for support, the court stated that the problem solved by the patents “does not alter the [court’s] analysis [because] ... nowhere do *the claims* reference the specific problem the SMS patents were designed to solve.” App. at 33a (emphasis added).

And when SMS argued that features recited in the claims were not routine, generic, or conventional, but instead were novel in 2001 when the applications for patents were filed, the court stated that “that is not the relevant inquiry at Step Two. Rather, the key question is whether the *underlying* ‘technology described in the patent [was] well-known at the time of the filing’” *Id.* at 40a. It is statements like this that suggest that courts are missing the forest for the trees.

While the court eventually addressed SMS’ argument that the claimed inventions would not preempt the identified abstract idea, substantially or otherwise, it did so in a single paragraph, at the end of the order, and in conclusory fashion. The court did not explain how a new and improved barcode that includes an identifier that is not assigned by the mail carrier, as traditionally done, but is assigned by the sender of the mail object, and is then concatenated with three other specific values in order to render the barcode globally unique, would preempt the highly generalized abstract idea of “communicating information about a mailpiece by use of a marking.”

In fact, while SMS, Defendant Universal Wilde (“UW”), and the United States Patent and Trademark Office (“USPTO”), identified several markings that have historically been used to communicate information about mailpieces, not one of them would have been preempted by the claimed inventions. Perhaps this is why the Federal Circuit choose to sidestep the issue of preemption (*see generally* at App. 1a-14a), which is strange since this Court has repeatedly stated that ***preemption*** is “***the concern that drives this exclusionary principle.***” *See, e.g., Alice*, 134 S. Ct. at 2354 (emphasis added).

In *Alice*, the Court stated that “in applying the § 101 exception, we must distinguish between patents that claim the ‘buildin[g] block[s]’ of human ingenuity and those that integrate the building blocks into something more.” *Id.* The Court went on to say that [t]he latter pose[s] no comparable risk of preemption, and therefore remain[s] eligible for the monopoly granted under our patent laws.” *Id.*

If preemption truly is the underlying concern, then courts should consider substantial preemption as objective evidence as to whether a claim includes an “inventive concept.” If the court finds that a claim substantially preempts the identified abstract idea, then the claim, by definition, is ineligible for patent protection. On the other hand, if the court finds that the claim would not substantially preempt the abstract idea identified in the first part of *Alice*, then it stands to reason that the claim includes an “inventive concept,” and is therefore eligible for patent protection.

Not only does this simplify the application of the

second part of *Alice*, but it avoids confusion between issues of inventiveness that are relevant to a § 101 analysis versus that for novelty and non-obviousness under 35 U.S.C. §§ 102 and 103.

STATEMENT OF THE CASE

I. THE INVENTION

The patents-in-suit describe and claim inventions that resulted from the anthrax attacks that took place shortly after the terrorist attacks of September 11, 2001. Anonymous letters laced with anthrax spores were sent to several media companies and congressional offices, resulting in five deaths and seventeen people being infected. As a result of these terrorist attacks, inventor Todd Fitzsimmons, President of SMS, began working on concepts for providing protection against unwanted and dangerous mailings and deliveries.

The concepts were constructively reduced to practice and filed as patent applications with the USPTO in late 2001. According to the patents, there are several problems with traditional mail services:

First, the mail object is typically secured inside packaging (*e.g.*, envelopes, 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. ... Second, a manual delivered mail object is limited to a one-way production of a finite set of information and/or products. This be-

comes problematic when the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.).

App. at 115a (1:29-56).

The inventions solved these problems by *allowing a sender of the mail object* (e.g., a secure mail receiving office, etc.) *to generate “mail ID data”* (i.e., a new and improved barcode) that is affixed to a mail object and uniquely identifies the mail object. *The mail ID data can then be used to provide*, for example, *authentication data from the sender* of the mail object *to the recipient* before the mail object is opened.

Because the invention could be used to fight terrorism, Mr. Fitzsimmons filed a “Petition for Special Application Status” with the USPTO, citing counter terrorism as the reason for special status. App. at 84a-86a. In granting the Petition, the USPTO stated:

Applicant’s declaration explains that the invention reduces the risk of terrorist attack by providing a system and method of verifying or authenticating a mail object before the mail object is opened and thereby minimizing the recipient’s exposure to the contents of the mail object by indicating that the mail object is safe to open or not safe to open via data comparison by the recipient from a secure facility. *This is an acceptable explanation of how the invention would act to counter terrorism.*

App. at 87a-88a (emphasis added).

A drawback in allowing the sender to provide information on the mail object *directly* to the recipient, *without involving the mail carrier*, lies with the sender creating an identifier for the mail object that is globally unique. This problem was explained before the Board of Patent Appeals and Interferences (“BPAI”) during prosecution of the patents:

The problem when you have a sender generating, or creating, the unique identifier is that there is no assurance that the identifier is indeed unique. You can imagine different senders using the same identifier on the same mail object, thus defeating the purpose. So the solution in the industry is to not allow the sender to generate, or create, the unique identifier. This is done by the mail carrier. So for example, if you go to FedEx, FedEx will generate a unique identifier or a tracking number. The same is true for UPS[,] Airborne, DHL, and so forth.

App. at 93a-94a.

One claimed solution is to use a barcode that includes four separate values concatenated together, where at least one of the values is assigned by the sender of the mail object. For example, Claim 1 of U.S. Pat. No. 7,818,268 provides “said mail identification data compris[es] ***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 said sender*** of said at least one mail object.” App. at 117a (6:20-26). This claim is exemplary of claims from U.S. Pat. Nos.

7,814,032 and 8,073,787, all of which were asserted against UW in this case.

This claimed solution was described before the BPAI during prosecution of the patents:

So the application solves the problem of how do you allow the sender to generate a unique identifier, and they [sic] also ensure that that identifier is truly unique enough to track or identify the mail object. And it does this by concatenating data onto the center-generated [sic] identifier. So for example, you can concatenate sender data, which would identify the sender of the mail object, onto the sender-generated identifier, and that would allow you to distinguish the mail object from objects sent by other senders. You could concatenate recipient data, which would allow you to distinguish the mail object from objects sent to different recipients. You could concatenate shipping data to distinguish mail objects that were sent on different dates from different locations, and so forth. In fact, *in one embodiment of the invention, the claims concatenate both sender data, recipient data, and shipping data onto the sender-generated identifier to create a truly unique identification number*, if you will.

App. at 94a (emphasis added).

Thus, a critical aspect of the invention is the non-conventional barcode, or single set of encoded data, that includes four separate values concatenated together, with at least one value assigned by the sender of the mail object. This was confirmed by Judge Lorin of the BPAI, who stated “[i]f I understand

what you’re saying, is that the distinctive aspect of your invention is this string, single set of encoded data, and that it includes a unique identifier, sender data, recipient data, and shipping method data?” App. at 102a. Mr. Fitzsimmons responded “Correct. Where the unique identifier is generated by the sender, correct.” *Id.*

Another claimed solution is to use ***a personalized network address***, such as a personalized Uniform Resource Locator (“pURL”), to uniquely identify the mail object. Not only is such an identifier, by definition, globally unique, but the identifier, itself, can be used to identify where on a network information on the mail object is stored. This “personalized network address” is recited in Claim 1 of U.S. Pat. No. 9,105,002. App. at 126a (6:35-54). This claim is exemplary of claims from U.S. Pat. Nos. 8,260,629, 8,429,093 and 8,910,860, all of which were asserted against UW in this case.

It should be noted that the ‘002 and ‘860 patents issued after the USPTO adopted guidelines consistent with the Court’s decision in *Alice*.

II. PROCEEDINGS BELOW

A. LOWER COURT PROCEEDINGS

In previous litigation, the district court construed certain claim limitations of the ‘268 and ‘787 patents in a Final Claim Construction Order. *See* App. at 54-83a. Therein, the district court construed several terms, including “sender data,” “recipient data,” “mail verification data,” and “verifying data.”

The district court started by noting that “the unique identifier must be assigned by the sender,

and that this is a crucial piece of the invention,” citing the hearing before the BPAI. App. at 70a. The court then held that “an entity or person who can be considered a ‘sender’ under the patent must be ‘indicated’ by the sender data and must also be the person or entity ‘who sent the mail object.’” App. at 71a-72a. The court also construed the claim term “recipient data” to mean “information indicating who is to receive the mail object, which may include the recipient’s address or account number” (App. at 72a) and the terms “mail verification data” and “verifying data” to mean “data from a mail verification application that is provided if there is correspondence between the verifying portion and the authenticating portion of the mail ID data” (App. at 78a).

In September 2015, SMS filed a complaint against UW for infringement of seven patents, including the two patents that were previously construed by the district court. The complaint summarized the patents and their prosecution histories, and copies of the patents were exhibits to the complaint. The complaint also provided specific examples of how UW was infringing exemplary claims from the patents in suit.

UW then filed a motion to dismiss the complaint under Rule 12 of the Federal Rules of Civil Procedure, arguing that SMS had failed to state a claim because all of its patent claims are invalid under 35 U.S.C. § 101. SMS opposed the motion. Among other points, SMS emphasized that UW had failed to properly perform either step of the two-step analysis mandated by the Supreme Court. With respect to the second part of the *Alice* test, SMS argued that UW “[i]gnor[ed] the most important and inventive as-

pects of th[e] patents' claims," and "there is no evidence that the patent-in-suit seek to preempt the performance of a fundamental business practice."

The district court granted UW motion, finding that all 234 claims of the seven patents-in-suit were directed to the same abstract idea (App. at 31a) and that the claims "do not contain the required inventive concept to save the SMS patents from ineligibility under § 101" (App. at 37a).

The court started by identifying the two-part analysis mandated by the Supreme Court. App. at 23a-25a. The court then explained that "[t]his [two-part analysis] is easier to articulate than it is to apply," that "[t]he line between a patentable 'process' and an unpatentable 'principle' is not always clear," and that "[p]inning down the exclusion for 'abstract idea' can be particularly challenging." *Id.*

With respect to the first part of the test, the court noted that "at Step One, "[c]ourts should recited a claim's purpose at a reasonably high level of generality." App. at 31a. As such, the court ignored critical features of the claimed inventions, and found that all 234 claims were directed to the abstract idea of "communicating information about a mailpiece by use of a marking." App. at 31a. However, describing claims at such a high level of abstraction and untethered from the language of the claims all but ensures that any claim can be characterized as directed to an abstract idea. This is because "all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract idea." Alice, 134 S. Ct. at 2354.

With respect to the second part of test, the court noted that the sender-generated barcode is “the core Step Two issue in this case.” App. at 39a. The court then went on to find that “this sender-generated barcode [is not] sufficiently inventive.” App. at 40a. This is because, according to the court, “the SMS patents simply rely on existing, well-known, technology.” *Id.* The court again ignored critical features of the claimed inventions,¹ stating that “the use of barcodes and other unique identifiers on piece of mail is not new,” and “the broad idea of communicating data through barcodes is used ubiquitously through postal tracking and the sending of electronic mail deliver receipts.” App. at 40a-41a.

While the court addressed the issue of preemption, it did so in a single paragraph, at the end of the opinion. Even though numerous mailpiece markings were identified in the record,² and not one of them would have been preempted by the claimed inventions, the court stated, in conclusory fashion, that “[b]ecause the asserted claims are not limited in any meaningful way, it raises significant concerns that the claims will preempt a large number of ways of

¹ As discussed above, Claim 1 of the ‘268 patent requires “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” (App. at 117a (6:20-26)), and Claim 1 of the ‘002 patent requires “said single set of mail ID data including ... a personalized network address associated with said recipient of said mail object” (App. at 126a (6:35-54)).

² This included markings identified in the prosecution history (*e.g.*, traditional tracking numbers created by mail carriers, iris data to uniquely identify the sender, etc.) and markings identified by UW (*e.g.*, the printing of a “skull and crossbones” or “fragile” on a mailpiece, etc.).

communicating information about a piece of mail by use of a marking.” App. at 52a.

B. FEDERAL CIRCUIT DECISION

SMS appealed the district court’s Order Granting Defendant’s Motion to Dismiss. With respect to *Alice* Step One, SMS argued that the District Court applied the wrong legal standard by “[f]ollowing the now-discarded approach of portraying claims at a high level of generality.” With respect to *Alice* Step Two, SMS argued that the district court failed to focus on claim elements, as required by *Alice*, and failed to properly consider whether the claimed inventions preempt the identified abstract idea. In particular, SMS argued that “[t]he concerns expressed by the district court about preemption were misplaced,” and “[t]he patent claims could not possibly preempt the broad abstract idea of ‘communicating information associated with a piece of mail by using of a marking’ as postulated by the district court.”

The issues were presented to Chief Judge Prost and Circuit Judges Clevenger and Reyna. Circuit Judge Reyna wrote the Federal Circuit Decision, affirm the district courts finding of ineligible subject matter. App. at 1a-14a. With respect to *Alice* Step One, the Federal Circuit stated that “the district court’s analysis correctly found that Secured Mail’s claims are directed to an abstract idea” (App. at 8a), and held that “the claims embrace the abstract idea of using a marking affixed to the outside of a mail object to communicate information about the mail object” (App. at 10a).

In discussing *Alice* Step Two, the court stated that while “the sender-generated identifier is created by combining various pieces of data, such as a unique identifier, sender data, recipient data and shipping method data ... [t]he *claim language* does not provide any specific showing of what is inventive about the identifier or about the technology used to generate and process it.” App. at 11a.

Despite SMS’ argument that the claimed inventions included an “inventive concept,” and that objective evidence of no preemption of the identified abstract idea is supportive of this finding, the Federal Circuit choose to side stepped the issue, and did not address the issue of preemption in their order. *See, e.g.*, App. at 1a-14a.

REASONS FOR GRANTING THE PETITION

I. CERTIORARI IS NEEDED TO ENSURE THAT THE UNDERLYING PRICIPLE OF PREEMPTION IS CONSIDERED WHEN DETERMINING WHETHER A CLAIM INCLUDES AN INVENTIVE CONCEPT

Preemption has repeatedly been described as the concern that drives the exclusionary principles for ineligible subject matter, such as laws of nature, natural phenomena, and abstract ideas.

In *Gottschalk v. Benson*, 409 U.S. 63 (1972), the Court considered whether one could patent the programming of a digital computer to convert signals from one form to another. The Court held that one could not, stating that “one may not patent an idea,” such as an algorithm, and that “the patent [at issue] would *wholly pre-empt* the mathematical formula and in practical effect would be a patent on the algo-

rithm itself.” *Id.* at 71-71 (emphasis added).

Preemption was again the issue in *Diamond v. Diehr*, 450 U.S. 175 (1981), where the claims were directed to a process for curing synthetic rubber. The Court held that the claims did constitute a “new and useful process” under 35 U.S.C. § 101 because “[while the] process admittedly employs a well-known mathematical equation ... **they do not seek to pre-empt the use of that equation.** Rather, they seek only to foreclose from others the use of that equation in conjunction with all of the other steps in their claimed process.” *Id.* at 187 (emphasis added).

Since those cases, preemption continues to come up on cases concerning patent eligible subject matter. In *Bilski v. Kappose*, 130 S.Ct. 3218 (2010), the Court stated:

The concept of hedging, described in claim 1 and reduced to a mathematical formula in claim 4, is an unpatentable abstract idea, just like the algorithms at issue in *Benson* and *Flook*. **Allowing petitioners to patent risk hedging would pre-empt use of this approach in all fields, and would effectively grant a monopoly over an abstract idea.**

Id. at 3231 (emphasis added). Similarly, in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 132 S.Ct. 1289 (2012), the Court begins the analysis by asking whether the “process is more than a drafting effort **designed to monopolize [i.e., preempt] the law of nature itself.**” *Id.* at 1297 (emphasis added).

In *Alice*, the Court began by acknowledging “the

concern that drives this exclusionary principle as **one of pre-emption.**” *Alice*, 134 S.Ct. at 2354 (emphasis added). The Court also acknowledged that courts must “tread carefully in construing this exclusionary principle lest it swallow all of patent law.” *Id.* Accordingly, the Court stated:

[I]n applying the § 101 exception, we must distinguish between patents that claim the “‘buildin[g] block[s]’ “ of human ingenuity and those that integrate the building blocks into something more, thereby “transform[ing]” them into a patent-eligible invention. The former “would risk disproportionately tying up the use of the underlying” ideas, and are therefore ineligible for patent protection. The latter pose **no comparable risk of pre-emption**, and therefore remain eligible for the monopoly granted under our patent laws.

Id. at 2354-2355 (emphasis added). The Court then stated that “[a] claim that recites an abstract idea, must include ‘additional features’ to ensure ‘that the [claim] is more than a drafting effort designed to monopolize [*i.e.*, preempt] the [abstract idea].” *Id.* at 2357. In *Alice*, the Court found the claim to implement an abstract idea on a generic computer. With respect to this, the Court stated:

Thus, if a patent’s recitation of a computer amounts to a mere instruction to “implement[t]” an abstract idea “on ... a computer,” that addition cannot impart patent eligibility. This conclusion accords with **the pre-emption concern that undergirds our § 101 jurisprudence.** Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of

“additional feature[e]” that provides any “practical assurance that the process is more than a drafting effort designed to ***monopolize [i.e., preempt] the [abstract idea] itself.***”

Id. at 2358 (emphasis added).

Given that preemption, or monopolization, of the abstract idea itself is the primary concern, it makes sense to begin the *Alice* Step Two analysis with a determination of whether the claim preempts, or has been drafted to monopolize, the abstract idea identified in *Alice* Step One. Not only would this provide courts with objective evidence of whether a claim includes an “inventive concept,” but it would safeguard against identifying abstract ideas that are untethered to the claim language.

As the Court noted, “[a]t some level, ‘all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas.’” *Id.* at 2354. In this case, the lower courts viewed the claims “at a reasonably high level of generality” (App. at 31a) in finding that the claims were directed to an abstract idea. In cases like this, the second part of *Alice* is the only safeguard preventing claims from falling victim to an overreaching of this exclusionary principle—a principle that “we [must] tread carefully in construing ... lest it swallow all of patent law.” *Alice*, 134 S. Ct. at 2354. By considering objective evidence of preemption, if a claim is truly monopolizing the identified abstract idea, then the claimed subject matter is ineligible for patent protection. On the other hand, if the claimed invention does not substantially preempt the identified abstract idea, then the claim, by definition, is entitled

to patent protection, assuming it meets the criterial of 35 U.S.C. §§ 102, 103, and 112.

Petitioner submits that certiorari is needed to ensure that the underlying principle of preemption is taken into consideration when determining whether a claim includes an “inventive concept.”

II. CERTIORARI IS NEEDED TO RESOLVE CONFLICTING APPROACHES TAKEN BY LOWER COURTS IN DETERMINING WHETHER A CLAIM INCLUDES AN IN- VENTIVE CONCEPT

As discussed above, the Federal Circuit failed to address the issue of preemption in determining whether the claims involved an “inventive concept.” *See generally* App. at 1a-14a. And while the district court included a single paragraph on preemption (App. at 52a), the analysis comes across as an afterthought, without any explanation as to why the claimed inventions, which required the concatenation of four specific values, including one sender-assigned value, into a single set of encode data (*e.g.*, a barcode), which is then compared to data previously stored in a database to authenticate a mail object, would substantially preempt the highly generalized abstract idea of “communicating information about a mailpiece by use of a marking.” Especially since markings identified in the record include the printing of a “skull and crossbones” or “fragile” on a mail object, and a traditional tracking number generated by a mail carrier.

Instead, the district court concluded that the claimed inventions do not include an “inventive concept” because they “rely on existing, well-known,

standard technology.” App. at 40a. However, according to the court, the “well-known, standard technology” includes “barcodes and other unique identifiers on pieces of mail.” *Id.* The court stated that “communicating data through barcodes is used ubiquitously through postal tracking and the sending of electronic mail delivery receipts.” App. at 40a-41a.

The problem with this analysis is that it completely ignores the claimed features that distinguish the claimed inventions over traditional postal tracking systems. The claimed inventions do not rely on “existing, well-known, standard technology,” and do not read on “the broad idea of communicating data through barcodes.” As discussed above, most of the claims require the concatenation of four specific values in order to render a sender-generated barcode globally unique. The other claims use a personalized network address to render a sender-generated barcode globally unique. Neither of these barcodes were “well-known at the time of filing or simply involved performance of ‘well-understood, routine, and conventional activities commonly used in the industry,’” as stated by the district court. App. at 40a.

In response to this argument, the court stated that “*even if* the sender-generated barcode (or other mail identification data) was a sufficiently inventive concept, the SMS patents ... lack specificity in describing the supposedly inventive concepts. As Defendant puts it, the SMS patents do not ‘disclose *how* the sender generates the information.’” App. at 42a-43a (emphasis in original). Thus, not only does the court’s § 101 analysis include inventiveness issues that are more properly addressed under 35 U.S.C. §§ 102 and 103, but it includes indefiniteness and writ-

ten description issues that are more properly addressed under 35 U.S.C. §112.

In all fairness, prior to applying the two-part test set forth by the Supreme Court, the district court noted that “[t]his standard is easier to articulate than it is to apply.” App. at 24a. The court went on to state:

“The line between a patentable ‘process’ and an unpatentable ‘principle’ is not always clear.” *Parker v. Flook*, 437 U.S. 584, 589 (1978). The Federal Circuit has referred to § 101 jurisprudence as a “murky morass.” *MySpace, Inc. v. GraphOn Corp.*, 672 F.3d 1250, 1259 (Fed. Cir. 2012) (suggesting, in dicta, that “courts could avoid the swamp of verbiage that is § 101” by addressing patentability defenses under §§ 102, 103, and 112 before addressing patent eligibility under § 101). Judge Pfaelzer recently lamented that “Supreme Court decisions on § 101 often more than clarify.” *California Inst. of Tech. v. Hughes Commc’ns Inc.*, 59 F. Supp. 3d 974, 80 (C.D. Cal. 2014); *see also MySpace, Inc.*, 672 F.3d at 1259 (“Our opinions spend page after page revisiting our cases and those of the Supreme Court, and still be continue to disagree vigorously over what is or is not patentable subject matter.”). Pinning down the exclusion for “abstract ideas” can be particularly challenging. *See MySpace, Inc.*, 672 F.3d at 1259 (“When it comes to explaining what is to be understood by ‘abstract ideas’ in terms that are something less than abstract, courts have been less than successful.”).

App. at 24a-25a.

Without guidance from the Court, courts will continue to issue decisions like this, where preemption is either not addressed, addressed as an afterthought, or addressed improperly by either not considering specific claim limitation or not comparing the claimed features to the identified abstract idea.

Petitioner submits that certiorari is needed to resolve conflicting, and inaccurate approaches taken by lower courts in determining whether a claim includes an “inventive concept.”

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

BY Todd Fitzsimmons
TODD E. FITZSIMMONS*
FITZSIMMONS IP LAW
P.O. Box 199
Gardena, CA 90248
(213) 500-1178

COUNSEL FOR PETITIONER

January 16, 2018

* Counsel of Record

**APPENDIX SUPPORTING THE
PETITION FOR A WRIT OF CERTIORARI**

United States Court of Appeals for the Federal Circuit

SECURED MAIL SOLUTIONS LLC,
Plaintiff-Appellant

v.

UNIVERSAL WILDE, INC.,
Defendant-Appellee

2016-1728

Appeal from the United States District Court for the
Central District of California in No. 2:15-cv-07562-DOC-
GJS, Judge David O. Carter.

Decided: October 16, 2017

WILLIAM J. O'BRIEN, One LLP, Beverly Hills, CA, ar-
gued for plaintiff-appellant.

GREGORY H. LANTIER, Wilmer, Cutler, Pickering, Hale
and Dorr LLP, Washington, DC, argued for defendant-
appellee. Also represented by ROBERT MANHAS.

Before PROST, *Chief Judge*, CLEVINGER, and REYNA,
Circuit Judges.

REYNA, *Circuit Judge*.

Secured Mail Solutions LLC appeals from the United States District Court for the Central District of California’s grant of a motion to dismiss on grounds that the claims of seven asserted patents are directed to subject matter ineligible for patenting under 35 U.S.C. § 101. Because the claims of the asserted patents are directed to an abstract idea and the claims contain no additional elements that transform the nature of the claims into a patent-eligible application of the abstract idea, we *affirm*.

BACKGROUND

This appeal involves seven patents that Secured Mail groups into three categories. U.S. Patent Nos. 7,814,032, 7,818,268, and 8,073,787 are the “Intelligent Mail Barcode” patents. U.S. Patent Nos. 8,260,629 and 8,429,093 are the “QR Code” patents. U.S. Patent Nos. 8,910,860 and 9,105,002 are the “Personalized URL” patents.

All the patents involve methods whereby a sender affixes an identifier on the outer surface of a mail object (e.g. envelope or package) before the mail object is sent. Computers and networks are used to communicate the information about the mail object’s contents and its sender after the mail object is delivered.

The Intelligent Mail Barcode patents recite a method for verifying the authenticity of the mail object. The identifier or barcode is a single set of encoded data that is generated by concatenating a sender-assigned unique identifier with sender data, recipient data, and shipping method data. ’268 patent, J.A. 76–77. The barcode is affixed to the outside of the mail object and an authenticating portion of the barcode is stored in a database. The recipient of the mail object can access the database and use that authenticating portion to verify that a mail object is authentic.

The QR Code and Personalized URL patents additionally require that a reception device (e.g., personal

computer) be used to scan the encoded data and display the resulting data on the reception device's display screen. *See, e.g.*, '629 patent, J.A. 98; '093 patent, J.A. 107; '860 patent, J.A. 120. In the QR Code patents, the identifier is a QR code (two-dimensional barcode) which a user can scan to look up additional electronic information related to the mail object. Specifically, the barcode includes data that allows the recipient of the mail object to request data directly from the sender and allows the sender to provide personalized data directly to the recipient, without the involvement of the mail carrier. For example, a customer might scan the QR code and be directed straight to her account rather than having to log in to access the account.

In the Personalized URL patents, a method similar to the QR Code patents is used, except the identifier is a personalized network address, or URL. For example, the user can type the URL into her web browser and be directed straight to a specific account, or to other personalized information. The types of data provided by the sender include content information, warranty information, and account information.

For the Intelligent Mail Barcode patents, claim 1 of the '268 patent is representative:

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.

J.A. 76 at col. 6 ll. 18–37.

For the QR Code patents, claim 1 of the '093 patent is representative:

1. A method for providing electronic data to a recipient of a mail object, comprising:

Generating, by a processor, a barcode for a mail object, said barcode including at least a first set of mail data, said first set of mail data including data corresponding to said recipient of said mail object;

affixing said barcode to said mail object;

submitting said mail object to a mail carrier for delivery to said recipient of said mail object;

receiving said first set of mail data, including data corresponding to said recipient of said mail object, from a reception device of said recipient via a network;

providing said electronic data to said reception device via said network in response to receiving said first set of mail data, said electronic data including a content of said mail object;

wherein said reception device displays said electronic data to a recipient of said mail object by displaying said electronic data on a screen of said reception device.

J.A. 107 at col. 6 ll. 22–40.

For the Personalized URL patents, claim 1 of the '860 patent is representative:

1. A method for providing electronic data to a recipient of a mail object, comprising:

using an output device to affix a single set of mail ID data to said mail object, said single set of mail ID data including at least recipient data, said recipient data comprising a personalized network address associated with said recipient of said mail object;

submitting said mail object to a mail carrier for delivery to said recipient of said mail object;

receiving said recipient data from a reception device of said recipient via a network; and

providing by at least one processor said electronic data to said reception device via said network in response to receiving said recipient data, said electronic data including data on a content of said mail object;

wherein said reception device displays said electronic data to a recipient of said mail object by displaying said electronic data on a screen of said reception device.

J.A. 120 at col. 6 ll. 34–51.

Universal moved to dismiss Secured Mail's complaint under Fed. R. Civ. P. 12(b)(6), arguing that Secured Mail's patents were not patent-eligible under Section 101. On February 16, 2016, the district court found that all seven

patents were directed to patent-ineligible subject matter. It reasoned that “the asserted claims, viewed individually or in combination, do not meaningfully limit the abstract idea of communicating information about a mailpiece by use of marking.” *Secure Mail Sols. LLC v. Universal Wilde, Inc.*, 169 F. Supp. 3d 1039, 1058 (C.D. Cal. 2016).

Secured Mail appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

STANDARD OF REVIEW

We review procedural questions that are not unique to patent law, such as a grant of a motion to dismiss for failure to state a claim, according to the law of the regional circuit, which in this case is the Ninth Circuit. *See, e.g., Univ. of Utah v. Max-Planck-Gesellschaft Zur Forderung Der Wissenschaften E.V.*, 734 F.3d 1315, 1319 (Fed. Cir. 2013). The Ninth Circuit reviews de novo a dismissal for failure to state a claim. *See, e.g., Livid Holdings Ltd. v. Salomon Smith Barney, Inc.*, 416 F.3d 940, 946 (9th Cir. 2005). This court also reviews a district court’s determination of patent eligibility under 35 U.S.C. § 101 de novo. *See, e.g., McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1311 (Fed. Cir. 2016).

DISCUSSION

The Patent Act defines patent-eligible subject matter as “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.” 35 U.S.C. § 101. The courts have created certain exceptions to the literal scope of § 101, determining that laws of nature, natural phenomena, and abstract ideas are not patent-eligible. *Alice Corp. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354 (2014) (quoting *Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)).

In *Alice*, the Supreme Court applied a two-step framework for analyzing whether claims are patent-

eligible under section 101. First, we determine whether the claims at issue are “directed to” a judicial exception, such as an abstract idea. 134 S. Ct. at 2355. If not, the inquiry ends. *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1346 (Fed. Cir. 2017); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016). If the claims are determined to be directed to an abstract idea we next consider under step two whether the claims contain an “inventive concept” sufficient to “transform the nature of the claim into a patent-eligible application.” *Alice*, 134 S. Ct. at 2355.

1. *Alice* Step One

Under *Alice* step one we consider the claims in their entirety to ascertain whether they are directed to ineligible subject matter. *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015). We look to whether the claims “focus on a specific means or method[, . . .] or are instead directed to a result or effect that itself is the abstract idea and merely invokes generic processes and machinery.” *McRO*, 837 F.3d at 1314 (citation omitted).

The district court found that the claims of all seven of the asserted patents “are directed to the abstract idea of communicating information about a [mail object] by use of a marking.” *Secured Mail*, 169 F. Supp. 3d at 1049.

On appeal, Secured Mail argues that its claims are patent-eligible under *Enfish*, an opinion issued after the district court’s decision in this case. In particular, the district court quoted the since-reversed district court decision in *Enfish* to hold that courts “should recite a claim’s purpose at a reasonably high level of generality.” *Secure Mail*, 169 F. Supp. 3d at 1048 (quoting *Enfish, LLC v. Microsoft Corp.*, 56 F. Supp. 3d 1167, 1173 (C.D. Cal. 2014), *rev’d*, 822 F.3d 1327 (Fed. Cir. 2016)). The Federal Circuit in *Enfish* held that the district court had described the claims at too high a level of abstraction, and

“describing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule.” 822 F.3d at 1337. Here, despite the district court’s statement that “a reasonably high level of generality” should be used, the district court’s analysis correctly found that Secured Mail’s claims are directed to an abstract idea.

The court in *Enfish* held the claims relating to a computer database implementation to be patent-eligible under *Alice* step one because the claims focused on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity. *Id.* at 1332–33. The claims in *Enfish* related to organization of data in a table in computer memory and a system for indexing that data. *Id.* at 1332–332. In contrast, the claims of Secured Mail’s patents are not directed to an improvement in computer functionality. For example, the claims are not directed to a new barcode format, an improved method of generating or scanning barcodes, or similar improvements in computer functionality.

Secured Mail argues that the claims are specifically directed to a sender-generated unique identifier, which improved on the existing process both by reliably identifying the sender of the mail object and by permitting the sender to create a bi-directional communication channel between the sender and recipient of the mail object. The fact that an identifier can be used to make a process more efficient, however, does not necessarily render an abstract idea less abstract.

The claims of the Intelligent Mail Barcode patents are not directed to specific details of the barcode or the equipment for generating and processing it. The claims generically provide for the encoding of various data onto a mail object but do not set out how this is to be performed. The claims state that various identifiers are affixed to a

mail object, stored in a database, scanned from the mail object, and retrieved from the database. No special rules or details of the computers, databases, printers, or scanners are recited. *Cf. McRO*, 837 F.3d at 1315 (finding patent eligibility where the “claimed process uses a combined order of specific rules that renders information into a specific format that is then used and applied to create desired results”); *Thales*, 850 F.3d at 1349 (finding patent eligibility where the “claims specify a particular configuration of inertial sensors and a particular method of using the raw data from the sensors”).

There is no description of how the unique identifier is generated or how a unique identifier is different from a personal name, or return address. Rather, the claim language cited by Secured Mail merely recites that the unique identifier is generated by the sender. The fact that the sender generates a barcode, which itself is not claimed, does not render the idea any less abstract.

The QR Code patents fare no better. The claims of these patents provide a method whereby a barcode is generated, affixed to a mail object, and sent through the mail system. Then, upon receipt, the barcode is scanned, and data corresponding to the sender is sent to the recipient over the network and displayed on the recipient’s device. This method is not limited to any particular technology of generating, printing, or scanning a barcode, of sending a mail object, or of sending the recipient-specific information over a network. Rather, each step of the process is directed to the abstract process of communicating information about a mail object using a personalized marking.

The Personalized URL patents are directed to the same abstract idea. The claims recite a personalized network address that is affixed to a mail object using an output device, the mail object is submitted to a mail carrier, and then once the mail object is received, a re-

quest is made by the recipient over the network using the personalized network address, and data is displayed on a screen. As with the other patents, each step of the process uses an identifier, in this case a personalized network address, to communicate information about a mail object.

The claims of the three sets of patents are not limited by rules or steps that establish how the focus of the methods is achieved. Instead, the claims embrace the abstract idea of using a marking affixed to the outside of a mail object to communicate information about the mail object, i.e., the sender, recipient, and contents of the mail object. Because the claims are directed to an abstract idea, we turn to the second step of the *Alice* inquiry.

2. *Alice* Step Two

In step two, we consider the elements of the claims to determine whether they transform the nature of the claim into a patent-eligible application of the abstract idea. *Content Extraction & Transmission LLC v. Wells Fargo Bank*, 776 F.3d 1343, 1347 (Fed. Cir. 2014). This is the search for an inventive concept, which is something sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. *Id.* “To save a patent at step two, an inventive concept must be evident in the claims.” *Recognicorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017). Merely reciting the use of a generic computer or adding the words “apply it with a computer” cannot convert a patent-ineligible abstract idea into a patent-eligible invention. *Versata Dev. Grp., Inc. v. SAP Am., Inc.*, 793 F.3d 1306, 1332 (Fed. Cir. 2015) (citing *Alice*, 134 S. Ct. at 2358).

Secured Mail argues that the district court misunderstood the step two analysis, and instead of searching for an inventive concept, it only asked whether the “underlying” technology was conventional. We disagree. The district court decision has pages analyzing the individual

claim elements concluding that the claims are “replete” with routine steps, including “affixing mail identification data,” such as a barcode, to a mail object or “submitting a mail object to a mail carrier for delivery.” *Secure Mail*, 169 F. Supp. 3d at 1051. The district court focused on the sender-generated barcode because Secured Mail argued that the sender-generated barcode was the inventive concept. The district court is correct to search for an inventive concept in precisely the factors that Secured Mail argues comprises the inventive concept. The district court addressed Secured Mail’s argument that “the development of a unique, sender-generated identifier *is* the critical invention.” *Id.* at 1052.

In the Intelligent Mail Barcode patents, the sender-generated identifier is created by combining various pieces of data, such as a unique identifier, sender data, recipient data and shipping method data. The data need not even be in the form of a barcode, much less a specific new type of barcode. The claim language does not explain how the sender generates the information, only that the information itself is unique or new. The claim language does not provide any specific showing of what is inventive about the identifier or about the technology used to generate and process it. The district court is correct that the sender-generated identifier is not a sufficiently inventive concept. *Id.* at 1051–53.

For the QR Code and Personalized URL patents, the district court concluded that there was no inventive concept. We agree. The claims merely provide that an identifier is affixed to a mail object that is used by the recipient to request and display electronic information. The use of barcodes was commonplace and conventional in 2001. *See, e.g.*, ’860 patent, J.A. 112–114 (citing references prior to 2001 regarding use of barcodes); *see also* ’032 patent, J.A. 65 at col. 3 ll. 28–34, col. 4 ll. 65–67 (noting that barcode scanners were generally known to those skilled in the art). In addition, sending a personal-

ized URL to a recipient was not an unconventional use of the Internet in 2001, for example, in emails that contained a personalized response URL. Nor is the “bi-directional communication line” inventive; the idea of responding to or inquiring about mail using a personalized identifier through the use of a marking (such as an account number printed on a utility bill, or a check number printed on a check) has long been a conventional concept.

Secured Mail analogizes to *DDR Holdings, LLC v. Hotels.com, L.P.*, which held claims that “specify how interactions with the Internet are manipulated to yield a desired result” and recite “a specific way to automate the creation of a composite web page by an ‘outsource provider’ that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet” are patent-eligible under section 101. 773 F.3d 1245, 1258–59 (Fed. Cir. 2014). The claims in Secured Mail’s patents are non-specific and lack technical detail. Rather than citing a specific way to solve a specific problem as in *DDR*, the asserted claims cite well known and conventional ways to allow generic communication between a sender and recipient using generic computer technology.

The fact that many of these technologies were well-known can be discerned from Secured Mail’s patents themselves. The patents mention that the invention can be performed using many types of hardware, including “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,” suggesting that the hardware used is conventional. ’032 patent, J.A. 65 at col. 3 ll. 29–34. The “Background of the Invention” section notes that contents that can be delivered electronically are often included in mail objects that are delivered via traditional mail services. ’032 patent, J.A. 64 at col. 1 ll. 50–52.

Some of the claim elements, such as submitting a mail object to a mail carrier or affixing information to a mail object, are routine to persons that have mailed a letter.

We see no inventive concept that transforms the nature of the claims into a patent-eligible application of the abstract idea.

Secured Mail argues that because the district court's conclusions address questions of fact, it was inappropriate for the district court to dismiss the case via Rule 12(b)(6). Yet, this court has determined claims to be patent-ineligible at the motion to dismiss stage based on intrinsic evidence from the specification without need for "extraneous fact finding outside the record." *See, e.g., In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 613–14 (Fed. Cir. 2016); *Content Extraction*, 776 F.3d at 1349; *cf. OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362 (Fed. Cir. 2015) (holding that a Section 101 inquiry is a question of law).

Secured Mail also argues that the district court erroneously shifted the burden of proof on the question of whether more than just industry-standard technology is claimed. According to Secured Mail, the district court improperly required it to prove that affixing a URL or barcode to a mail object was unconventional. Secured Mail's argument is misplaced. In ruling on a 12(b)(6) motion, a court need not "accept as true allegations that contradict matters properly subject to judicial notice or by exhibit," such as the claims and the patent specification. *Anderson v. Kimberly-Clark Corp.*, 570 F. App'x 927, 931 (Fed. Cir. 2014) (quoting *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001)). Here, the district court did not place any special burden of proof on Secured Mail, but simply concluded from the claims that they were directed to patent-ineligible subject matter.

CONCLUSION

For the foregoing reasons, we *affirm* the district court's grant of Universal's motion to dismiss.

AFFIRMED

COSTS

No costs.

**ORDER GRANTING DEFENDANT'S
MOTION TO DISMISS
(FEBRUARY 16, 2016)**

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SECURED MAIL SOLUTIONS LLC

Plaintiff,

v.

UNIVERSAL WILDE, INC.

Defendant.

Case No. CV 15-7562-DOC (GJSx)

Re: Dkt. No. 24

Before: David O. CARTER
United States District Court Judge

Before the Court is Defendant Universal Wilde, Inc.'s ("Defendant" or "UW") Motion to Dismiss ("Motion") (Dkt. 16). The Court finds this matter appropriate for resolution without oral argument. Fed. R. Civ. P. 78; L.R. 7-15. Having reviewed the moving papers and considered the parties' arguments, the Court hereby GRANTS Defendant's Motion.

I. Background

In its Complaint (“Compl.”) (Dkt. 1), Plaintiff Secure Mail Solutions LLC (“Plaintiff” or “SMS”) asserts claims of patent infringement of seven related patents: U.S. Patent No. 7,814,032 (“the ‘032 patent”), issued on October 12, 2010; U.S. Patent No. 7,818,268 (“the ‘268 patent”), issued on October 19, 2010; U.S. Patent No. 8,073,787 (“the ‘787 patent”), issued on December 6, 2011; U.S. Patent No. 8,260,629 (“the ‘629 patent”), issued on September 4, 2012; U.S. Patent No. 8,429,093 (“the ‘093 patent”), issued on April 23, 2013; U.S. Patent No. 8,910,860 (“the ‘860 patent”), issued on December 16, 2014; and U.S. Patent No. 9,105,002 (“the ‘002 patent”), issued on August 11, 2015. Collectively, the Court will refer to these patents as the “SMS patents.” In total, there are 234 claims in the SMS patent, and Plaintiff asserts 143 of them against UW. Opp’n at 1. Plaintiff highlights four of the claims in its Complaint. Mot. at 6; *See generally* Compl.

The inventor and president of SMS, Todd Fitzsimmons (“Fitzsimmons”), developed the idea for these second patents after the events of September 11, 2011. Declaration of Todd Fitzsimmons (“Fitzsimmons Decl.”) (Dkt. 21-1) ¶¶ 2-3. Mr. Fitzsimmons imagined that the patented system could protect mail recipients from possible anthrax or explosive attacks by mail because the system would permit recipients to verify the source of the package before opening it. *Id.* ¶¶ 3-4. SMS asserts that these inventions have greatly improved the “safety and security of mail.” *See* Compl. ¶ 8.

A. The IMb Patents

SMS refers to the ‘032 patent, ‘268 patent, and ‘787 patent as the “IMb Patents.” Opp’n at 5. These three patents “claim subject matter that includes a novel barcode, which has since been adopted by the United States Postal Service, and is referred to as the Intelligent Mail barcode.” Fitzsimmons Decl. ¶ 7.

Claim 1 of the ‘268 patent, which is featured in the Complaint, reads as follows:

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.

Compl. ¶ 10; See ‘268 Patent at Col. 6:18-37.

The abstract of the ‘268 patent states in full:

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.

‘268 Patent Abstract.

B. The Personalized QR Code Patents

SMS refers to the '629 and '093 patents as the "Personalized QR Code patents." Opp'n at 5. SMS states that these two patents "claim a barcode that has been personalized for the recipient of the mail piece." *Id.*

Claim 1 of the '093 patent, which Plaintiff cites to in the Complaint, provides:

A method for providing electronic data to a recipient of a mail object, comprising:

Generating, by a processor, a barcode for a mail object, said barcode including at least a first set of mail data including data corresponding to said recipient of said mail object;

affixing said barcode to said mail object;

submitting said mail object to a mail carrier for delivery to said recipient of said mail object;

receiving said first set of mail data, including data corresponding to said recipient of said mail object, from a reception device of said recipient via a network;

wherein said reception device displays said electronic data to a recipient of said mail object by displaying said electronic data on a screen of said reception device.

Compl. ¶ 18; '093 Patent at Col. 6:22-40. The abstract of the '093 patent is substantially similar to the abstract of the '268 patent. *See* '093 Patent Abstract.

C. The pURL Patents

Plaintiff contends that the two remaining patents-in-suit – the ‘860 patent and the ‘002 patent – “claim mail identification data that has been personalized for the recipient of the mail piece (using, for example, a personalized network address) and thus cover (among other things) a ‘personalized uniform resource locator, or pURL” Opp’n at 5.

In its Complaint, SMS highlights Claim 1 of the ‘002 patent, which states:

A method for providing electronic data to a recipient of a mail object, comprising:

using an output device to affix a single set of mail ID data to said mail object, said single set of mail including at least recipient data, said recipient data comprising a personalized network address associated with said recipient of said mail object;

submitting said mail object to a mail carrier for delivery to said recipient of said mail object;

receiving said recipient data from a reception device of said recipient via a network; and

providing by at least one processor said electronic data to said recipient device via said network in response to receiving said recipient data, said electronic data comprising a sender web page that identifies said recipient of said mail object and includes data corresponding to a content of said mail object;

wherein said electronic data is configured to be displayed to said recipient via a web browser on a display of said reception device.

Compl. ¶ 26; ‘002 Patent at Col. 6:35-54. The abstract for the ‘002 patent is substantially similar to the abstract of the ‘268 abstract quoted above.

D. Procedural History

On April 8, 2014, in a separate litigation, this Court issued a Claim Construction in which it construed four terms of the ‘268 patent and the ‘787 patent. *See* Final Order on Claim Construction (“Claim Construction Order”) (Dkt. 195), *Secured Mail Solutions LLC v. Advanced Image Direct LLC et al.*, Case No. SA CV 12-1090-DOC (RNBx). In the Claim Construction Order, the Court construed four terms in the ‘268 and ‘787 patents: (1) “sender” and related terms; (2) “recipient” and related terms; (3) “mail verification data” and “verifying data”; and (4) “mail verification device.”

Plaintiff filed the instant suit on September 25, 2015 (Dkt. 1). The case was transferred to this Court on September 20, 2015 (Dkt. 11).

Defendant filed the instant Motion on November 23, 2015. Plaintiff opposed on December 7, 2015 (Dkt. 21), and Defendant replied on December 14, 2015 (Dkt. 22).

II. Legal Standard

A. Standard Under 12(b)(6)

Under Federal Rule of Civil Procedure 12(b)(6), a complaint must be dismissed when a plaintiff’s allegations fail to set forth a set of facts which, if true, would entitle the complaintant to relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Askcroft v. Iqbal*, 556 U.S. 662, 679 (2009) (holding that a claim must be facially plausible in order to survive a

motion to dismiss). The pleadings must raise the right to relief beyond the speculative level; a plaintiff must provide “more than labels and confusions, and a formulaic recitation of the elements of a cause of action will not do.” *Twombly*, 550 U.S. at 555 (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). On a motion to dismiss, this court accepts as true a plaintiff’s well-pleaded factual allegations and construes all factual inferences in the light most favorable to the plaintiff. See *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). The court is not required to accept as true legal conclusions couched as factual allegations. *Iqbal*, 556 U.S. at 678.

In evaluating a Rule 12(b)(6) motion, review is ordinarily limited to the contents of the complaint and material properly submitted with the complaint. *Van Buskirk v. Cable News Network, Inc.*, 284 F.3d 977, 980 (9th Cir. 2002); *Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc.*, 896 F.2d 1542, 1555 n.19 (9th Cir. 1990). Under the incorporation by reference doctrine, the court may also consider documents “whose content are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleadings.” *Branch v. Tunnell*, 14 F.3d 449, 454 (9th Cir. 1994), *overruled on other grounds by Galbraith v. Cnty. Of Santa Clara*, 307 F.3d 1119, 1121 (9th Cir. 2002). The court may treat such a document as “part of the complaint, and thus may assume that its contents are true for purposes of a motion to dismiss under Rule 12(b)(6).” *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).

Dismissal with leave to amend should be freely given “when justice so requires.” Fed. R. Civ. P. 15(a)(2). This policy is applied with “extreme liberality.” *Morongo Band of Mission Indians v. Rose*, 893 F.2d 1074, 1079 (9th Cir. 1990); *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (holding that dismissal with leave to amend should be granted even if no request to amend was made). Dismissal without leave to amend is appropriate only when the court is satisfied that the deficiencies in the complaint could not be cured by amendment. *Jackson v. Carey*, 353 F.3d 750, 758 (9th Cir. 2003).

B. Patent Eligibility Under 35 U.S.C. § 101

Section 101 of the Patent Act provides that a patent may be obtained for “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.” 35 U.S.C. § 101. The Supreme Court has “long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.” *Alice Corp. Pty. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354, 189 L. Ed. 2d 296 (2014). “The concern that drives this exclusionary principle” is “one of pre-emption.” *Id.* In other words, the concern is “that patent law not inhibit further discovery by improperly tying up the future use of these building blocks of human ingenuity,” *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1301, 182 L. Ed. 2d 321 (2012)). *Alice* warns courts, however, to “tread carefully in construing this exclusionary principle lest it swallow all of patent law,” because “[a]t some level, ‘all inventions ... embody, use, reflect, rest upon, or

apply laws of nature, natural phenomena, or abstract ideas.” *Id.* (quoting *Mayo*, 132 S. Ct. at 1293).

In *Alice*, the Court followed the framework it established in *Mayo* “for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.” *Id.* at 2355. First, the court asks “whether the claims at issue are directed to one of those patent-ineligible concepts.” *Id.* If so, the court then “consider[s] the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Id.* (quoting *Mayo*, 132 S. Ct. at 1298, 1297). In this second step, the court looks for an “inventive concept”—that is, “an element or combination of elements that is ‘sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.’” *Id.* (quoting *Mayo*, 132 S. Ct. at 1294).

This standard is easier to articulate than it is to apply. “The line between a patentable ‘process’ and an unpatentable ‘principle’ is not always clear.” *Parker v. Flook*, 437 U.S. 584, 589 (1978). The Federal Circuit has referred to § 101 jurisprudence as a “murky morass.” *MySpace, Inc. v. GraphOn Corp.*, 672 F.3d 1250, 1259 (Fed. Cir. 2012) (suggesting, in dicta, that “courts could avoid the swamp of verbiage that is § 101” by addressing patentability defenses under §§ 102, 103, and 112 before addressing patent eligibility under § 101). Judge Pfaelzer recently lamented that “Supreme Court decisions on § 101 often confuse more than they clarify.” *California Inst. of Tech. v. Hughes Commc’ns Inc.*, 59 F. Supp. 3d

974, 80 (C.D. Cal. 2014); *see also MySpace, Inc.* 672 F.3d at 1259 (“Our opinions spend page after page revisiting our cases and those of the Supreme Court, and still we continue to disagree vigorously over what is or is not patentable subject matter.”). Pinning down the exclusion for “abstract ideas” can be particularly challenging. *See MySpace, Inc.*, 672 F.3d at 1259 (“When it comes to explaining what is to be understood by ‘abstract ideas’ in terms that are something less than abstract, courts have been less than successful.”).

C. Ripeness of Deciding Patent Eligibility, Defendant’s Burden, and Representative Claims

“Patent eligibility under § 101 is a question of law that may, in appropriate cases, be decided on the pleadings without the benefit of a claims construction hearing.” *Modern Telecom Sys. LLC v. Earthlink, Inc.*, No. SA CV 14-0347-DOC (ANx), 2015 1239992, at *6 (C.D. Cal. Mar. 17, 2015); (affirming district court’s decision to grant motion to dismiss based on patent ineligible subject matter under § 101 without having a claim construction hearing); (citing *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass’n*, 776 F.3d 1343, 1349 (Fed. Cir. 2014)); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 711 (Fed. Cir. 2014) (same).

The Court notes that it previously construed several of the claims at issue in a prior matter. *See generally* Claim Construction Order. Further, Plaintiff does not argue that additional claim construction is

necessary.¹ See *Open Text S.A. v. Alfresco Software Ltd*, Case No. 13-cv-04843-JD, 2014 WL 4684429, at *3 (N.D. Cal. Sept. 9, 2014) (“[T]his lack of dispute over the proper construction of the asserted claims confirms that it is unnecessary to engage in claim construction of the asserted claims confirms that it is unnecessary to engage in claim construction before addressing validity under Section 101.”). Therefore, the Court concludes that “[s]eparate claim construction proceedings are therefore not necessary to determine” patent eligibility. *Boar’s Head Corp. v. DirectApps, Inc.*, No. 2:14-cv-01927-KLM-KJN, 2015 WL 4530596, at *8 (E.D. Cal. July 28, 2015).

Additionally, the Court notes that “Defendants’ burden in seeking to dismiss plaintiff’s claim based on patent ineligibility is high because of the Patent’s presumptive validity.” *Boar’s Head Corp.*, 2015 WL 4530596, at *3. “[I]n applying § 101 jurisprudence at the pleading stage, the Court construes the patent claims in a manner most favorable to Plaintiff.” *Modern Telecom*, 2015 WL 1239992, at *8 (citing *Content Extraction*, 776 F.3d at 1349).

Finally, the Court recognizes the parties’ dispute concerning whether and how the Court should use representative claims. Plaintiff argues that Defendant improperly “lumps together all of the IMb Patents, Personalized QR Code Patents, and pURL Patents” and therefore “Defendant has failed to address the many differences between SMS’s seven patents and the hundreds of claims of those patents.” Opp’n at 9. Defendant responds that it is well established

¹ Plaintiff instead argues that Defendant’s “analysis is fatally flawed by its failure to recognize important limitations in SMS’s claims as construed by the Court.” Opp’n at 1.

that “courts need not analyze each and every asserted claim with the same degree of precision.” Mot. at 6 n.6. Defendant further argues that it simply analyzed the four “representative claims that *SMS* identified in its complaint” Reply at 9.

The Court agrees with Defendant that it is well-established that courts do not need to assess every claim in conducting a § 101 analysis. *See CMG Fin. Servs. v. Pac. Trust Bank, F.S.B.i*, 50 F. Supp. 3d 1306, 1314 (C.D. Cal. 2014) (citation omitted) (“Comparing the language of the systems claims with that of the method claims, it is clear that these are functionally identical ... Thus, they must be treated as equivalent for purposes of the § 101 analysis.”); *see also Bascom Research, LLC v. LinkedIn, Inc.*, 77 F. Supp. 3d 940, 943 n.3 (N.D. Cal 2015) (“Defendants assert, and the Court agrees, that claim 45 of the ‘974 patent is representative of the asserted claims.”). Here, the Court finds that the four claims included Plaintiff’s complaint are sufficiently similar to the other asserted claims to warranting treating them as “representative” for purposes of the § 101 analysis.² In any event, the Court, where necessary, still evaluates Plaintiff’s arguments that other specific “claims include features that either add to the patentability or are themselves patentable.” Opp’n at 9.

III. Discussion

In its Motion, Defendant argues that each of the asserted claims of the seven patents are not patent-eligible under § 101 because the claims “are all di-

² The four claims are: claim 1 of the ‘268 patent, claim 1 of the ‘093 patent, claim 1 of the ‘002 patent, and claim 1 of the ‘860 patent.

rected to the abstract idea – communicating information associated with a mailpiece by use of a marking on the mail’s packaging,” Mot. at 1, and because Plaintiff has failed to supply any inventive concept, *id.* at 18, Plaintiff responds that Defendant “has failed to properly perform the first step of the analysis mandated by the Supreme Court” and that the claims at issue “are replete with inventive features.” Opp’n at 2.

A. Step One of the *Mayo* Test

Under the first step of the *Mayo* test, the Court must determine whether the patent claims at issue are directed to abstract ideas. As an initial matter, the Court notes that, “identifying the precise nature of the abstract idea” to which Plaintiff’s patent claims are directed “is not straightforward as in *Alice* or some of [the Federal Circuit’s] other recent abstract idea cases.” *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014). Although there is some disagreement among courts as to how expansively a claim should be examined at Step One of the *Mayo* test, the Federal Circuit and the courts in this district instruct courts to examine the *purpose* of a challenged claim to determine whether it is directed to an abstract idea. *See California. Inst. Tech.*, 59 F. Supp. 3d at 991-92 (requiring that a court “identify the purpose of the claim—in other words, what the claimed invention is trying to achieve—and ask whether that purpose is abstract,” making the *Mayo* step 1 “a sort of ‘quick look’ test, the object of which is to identify a risk of preemption and ineligibility”).

For example, the claims in *Alice* were directed to the abstract idea of intermediate settlement, “i.e., the use of a third party to mitigate settlement risk,” and “simply instruct[ed] the practitioner to implement the abstract idea ... on a generic computer.” *Alice*, 134 S. Ct. at 2356, 2359. In *Ultramercial*, 772 F.3d at 715, the claims were directed to the abstract idea of “using advertisement as an exchange or currency.” In *buySAFE, Inc. v. Google Inc.*, the claims simply invoked a generic computer to implement the abstract concept of “creating a contractual relationship—a ‘transaction performance guaranty’—that is beyond question of ancient lineage.” 765 F.3d 1350, 1355 (Fed. Cir. 2014). In *Content Extraction*, the claims were “drawn to the abstract idea of 1) collecting data, 2) recognizing certain data within the collected data set, and 3) storing that recognized data in memory.” 776 F.3d at 1347. In *Digitech Image Technologies, LLC v. Electronics for Imaging, Inc.*, the claims simply recited “a process of taking two data sets,” which were “generated by taking existing information ... and organizing this information into a new form” and “combining them into a single data set.” 758 F.3d 1344, 1351 (Fed. Cir. 2014).

Here, Defendant argues that “[a]ll claims of the Secured Mail Patents are directed to the abstract idea of communicating information associated with a mailpiece by use of marking on the mail’s packaging.” Mot. at 13. Defendant references claim 1 of the ‘093 patent, which encompasses a “method of providing electronic data to a recipient of a mail object” in part by “generating a barcode including data corresponding to the recipient of the mail object.” *Id.* at 13-14; see ‘093 Patent at Col. 6:22-27. Thus, Defend-

ant argues the SMS patents are “directed to nothing more than communicating information about the contents of the mailpiece through use of a marking (a barcode) affixed to the mailpiece.” *Id.* at 14. In response, Plaintiff argues the SMS patents are directed to more than a mere abstract idea because they refer to a “sender-based system that is configured to send data identifying the recipient of the mail piece and data corresponding to the content of the mail piece.” Opp’n at 14.

The Court agrees that Defendant’s position better captures the nature of the asserted claims, and accordingly finds that the claims are directed to an abstract idea. The abstract of *each* of the seven SMS patents states that, “mail ID data is [] affixed to a mail object,” which allows for the “transmi[ssion] [of] information over a wide area network.” *See, e.g.*, ‘268 Patent. “Moreover, the patents’ recited purpose is consistent with the language of the claims.” *GT Nexus, Inc. v. Inttra, Inc.*, Case No: C 11-02145-SBA, 2015 WL 6747142, at *4 (N.D. Cal. Nov. 5, 2015) (quotation omitted). For instance, claim 1 of the ‘002 patent provides: “A method for providing electronic data to a recipient of a mail object, comprising: using an output device to affix a single set of mail ID data to said mail object.” ‘002 Patent at Col. 6:35-37.

The Court finds that attaching “mail ID data” to a piece of mail – which is often accomplished, for example, by using a barcode – that transmits information about that piece of mail to a recipient is directed to the abstract idea of communicating information associated with a mailpiece by use of a marking. This finding is further supported by looking to the names of the asserted patents – in particular,

the ‘093, ‘860, and ‘002 patents, which are labeled “System and Method for Providing Information to a Recipient of a Physical Mail Object.”³ See ‘093 Patent; ‘860 Patent; ‘002 Patent. Therefore, the Court finds that each of the SMS patents are directed to the abstract idea of communicating information about a mailpiece by use of a marking.

Plaintiff “does not meaningfully challenge this assertion in its opposition.” *Netflix, Inc. v. Rovi Corp.*, Case No. 11-cv-6591 PJH, 2015 WL 4345069, at *9 (N. D. Cal July 15, 2015). Fundamentally, Plaintiff fails to “offer any alternative characterization of the idea underlying its claim.” *Gametek LLC v. Zynga, Inc.*, CV 13-2546 RS, CV-13-3089-RS, CV-13-3472-RS, CV-13-3493-RS, 2014 WL 1665090, at *4 (N.D. Cal. Apr. 25, 2014). Instead, Plaintiff either misunderstands or attempts to sidestep the Step One analysis by repeatedly emphasizing the inventiveness of its asserted patents. See Opp’n at 13 (“UW ignores this aspect of the invention, which is not only an inventive aspect itself, but is how the sender-based system can authenticate the mail piece, and how the sender-based system can open a bi-directional communication channel with the recipient, thereby allowing other mail-related information to be provided.”). These arguments are irrelevant at Step One. See *Ultramercial*, 772 F.3d at 715. Plaintiff also takes issue with Defendant’s “broad portrayal of the patents,” Opp’n at 12, but of course, at Step One, “[c]ourts should recite a claim’s purpose at a reasonably high level of generality.” *Enfish, LLC v.*

³ The ‘032, ‘268, and ‘787 patent are titled “System and Method for Mail Verification,” and the ‘629 patent is titled “System and Method for Providing an Advertisement to a Recipient of a Physical Mail Object.”

Microsoft Corp., 56 F. Supp. 3d 1167, 1173 (C.D. Cal. 2014); *see also Open Text S.A. v. Box, Inc.*, 78 F. Supp. 3d 1043, 1046 (N.D. Cal. 2015) (noting that in evaluating the first prong of the Mayo test, “the Court distills the gist of the claim.”).

Finally, Plaintiff argues that because the SMS patents describe “concrete technological features and processes,” they cannot be directed to an abstract idea. *See* Opp’n at 13. This argument is also misguided. The claims at issue repeatedly refer to generic technological components, such as “mail verification device,” “reception device,” a “processor,” and “database.” *See, e.g.*, ‘268 Patent at Col. 6:29-31) (“at least a portion of the mail verification data is sent to the reception device”); *id.* at Col. 8:65-67 (“at least one *mail verification device* adapted to communicate with at least one *reception device* via network”) (emphasis added); ‘002 Patent at Col. 8:13-15 (“a *processor*; at least one application operating on at least *said processor*”) (emphasis added). As several courts have recognized, the generic reference to technological components is largely irrelevant to the Step One analysis. *See California Inst. of Tech.*, 59 F. Supp. 3d 974 at 993 (“Courts must ignore generic recitation of hardware at step one, when the claimed hardware essentially performs a method.”); *see also Enfish*, 56 F. Supp. 3d at 1176 (“When a claim recites a computer generically, the Court should ignore this element in defining the claim’s purpose.”) (citing *Alice*, 134 S. Ct. at 2356-57 (defining the claims purpose as intermediated settlement, not achieving intermediated settlement on a computer)). The Court adds that the claims’ reference to a network “does not save the claim from abstraction.” *See Intellectual*

Ventures 1 LLC v. Mfrs & Traders Trust Co., 792 F.3d 1363, 1366 (Fed. Cir. 2015) (“An abstract idea does not become nonabstract by limiting the invention to a particular field of use or technological environment, such as the Internet.”).

Additionally, the Court notes Plaintiff’s argument that the SMS patents are directed at solving a specific problem does not alter the analysis. For one, nowhere do the claims reference the specific problem the SMS patents were designed to solve. *OpenTv, Inc. v. Apple, Inc.*, Case No. 14-cv-01622-HSG, 2015 WL 1535328, at *4 (N.D. Cal. Apr. 6, 2015) (“[N]owhere do the ‘799 Patent claims say anything about ‘malicious eavesdropping’ or ‘interactive information systems’ ... On their face, then, the claims do not say what OpenTV claims they say.”). Even more, solutions to the problem of securing and communicating information about mail predate Plaintiffs’ patents. *See id.* (“The problem of how to transmit, receive, store, and organize confidential information deriving from multiple sources is not a creature of the Internet age: solutions to this problem date back to the invention of smoke signals.”). In *OpenTv, Inc. v. Apple, Inc.*, the court considered plaintiff’s argument that the patent at issue was “not directed to an abstract idea because it described a specific solution to overcome a technological problem that arose in the realm of electronic communications for interactive information systems, such as interactive televisions.” Case No. 14-cv-01622-HSG, 2015 WL 1535328, at *4 (N.D. Cal. Apr. 6, 2015) (internal quotation marks and citations omitted). The *OpenTv* court handily rejected this argument, finding, “the problem of transmitting confidential infor-

mation using unsecured communication methods has existed for centuries, long before the advent of interactive television networks. The ‘799 Patent claims are drawn to the abstract idea of using identification codes to solve this age-old problem.” *Id.* at *5 (citing *Planet Bingo, LLC v. CKGS LLC*, 576 Fed. App’x 1005, 1006-07 (Fed. Cir. 2014) (holding that claims were directed to the abstract idea of preventing “tampering problem[s]” and “other security risks” during commercial transactions) (internal quotation marks and citations omitted). The same is true here. Thus, the fact that the SMS patents were designed with a specific problem in mind does not change the outcome of the above Step One analysis.

For the reasons stated above, the Court concludes the SMS patents are directed to an abstract idea. Accordingly, the Court turns to the second prong of the patent eligibility inquiry.

B. Step Two of the *Mayo* Test

Having concluded the SMS patents are directed to the abstract idea of communicating information associated with a mailpiece by use of a marking, the Court now “examine[s] the limitations of the claims to determine whether the claims contain an ‘inventive concept’ to ‘transform’ the claimed abstract idea into patent-eligible subject matter.” *Ultramercial*, 772 F.3d at 715 (quoting *Alice*, 134 S. Ct. at 2357).

Under the second step of the *Mayo* test, the Court considers whether the elements of each claim, either individually or “as an ordered combination,” include an “inventive concept” such that “the patent in practice amounts to significantly more than a patent up-

on the [ineligible concept] itself.” *Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1294). “A claim that recites an abstract idea must include ‘additional features’ to ensure ‘that the [claim] is more than a drafting effort designed to monopolize the [abstract idea].” *Alice*, 134 S. Ct. at 2357 (quoting *Mayo*, 132 S. Ct. at 1297) (alterations in original). “Those ‘additional features’ must be more than ‘well-understood, routine, conventional activity.” *Ultramercial II*, 772 F.3d at 715 (quoting *Mayo*, 132 S. Ct. at 1298). As the “Supreme Court and the Federal Circuit have made it perfectly clear, merely implementing an abstract idea on conventional computer technology is not enough.” *IPLearn-Focus, LLC v. Microsoft Corp.*, Case No. 14-cv-00151-JD, 2015 WL 4192092, at *4 (N.D. July 10, 2015).

It is important to note that “the search for an ‘inventive concept’ places no importance on the novelty of the abstract idea. A novel abstract idea is still an abstract idea, and is therefore unpatentable.” *Netflix*, 2015 WL 4345069, at *7; *see also IpLearn, LLC v. K12 Inc.*, 76 F. Supp. 3d 525, 534 (D. Del. 2014) (“A new idea, i.e., one that is non-anticipated and non-obvious, does not, however, make an abstract idea patent eligible.”); *see also Bilski v. Kappos*, 561 U.S. 593, 610-11 (2010) (“[T]he fact that a company may be the first to successfully apply an abstract idea within a new technological context does not transform the abstract idea into something tangible and patentable.”). Further, “even if a claim does not wholly pre-empt an abstract idea, it still will not be limited meaningfully if it contains only insignificant or token pre or post-solution activity—such as identifying a relevant audience, a category of use, field of

use, or technological environment.” *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 1335, 1346 (Fed. Cir. 2013).

Defendant contends the SMS patents fail Step Two of the *Mayo* test because “[n]one of the remaining elements of the claims, alone or in combination, adds an inventive idea that would render them patent eligible.” Mot. at 17. Defendants specifically argue that the claim elements “all consist of hardware that was known in the art at the time of filing;” the claim consists of “conventional computing components (or humans) acting in conventional ways;” the patents provide no explanation on how the claimed limitations are accomplished; and the remaining limitations of the SMS patents add no inventive concepts. Mot. at 18-19, 21-22.

In response, Plaintiff asserts the “evidence shows that SMS’s claims include several significant inventive concepts, including solutions to solve several problems in the mailing and shopping industry and safety problems.” Opp’n at 14. According to Plaintiff, the most critical inventive concept “in the IMb Patents is the sender-generated barcode,” which provides 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.” *Id.* at 15 (citing ‘268 Patent at Col. 6:21-26). Plaintiff notes the “inventions of the IMb Patents may seem conventional now, but they were highly inventive in 2001.” *Id.* at 17. Plaintiff contends the QR Code Patents

and pURL Patents “contain still further inventive concepts.” *Id.*⁴

1. Initial Concerns

After a review of the SMS patents, the Court finds that the asserted “claims do not contain the required inventive concept to save the” SMS patents from ineligibility under § 101. *See Open Tv*, 2015 WL 1535328, at *5. As an initial matter, the majority of the steps of the asserted claims comprise the abstract concept of communicating information about a mailpiece by using a marking. *See id.* at 715-16. “Adding routing additional steps” does not transform an otherwise abstract idea into patent-eligible subject matter. *Ultramercial*, 772 F.3d at 716. The claims at issue here are replete with such steps, including “affixing mail identification data,” such as a barcode, to a piece of mail or “submitting said mail object to a mail carrier for delivery.” *See, e.g.*, ‘268 Patent at Col. 6:20; ‘093 Patent at Col. 6:29. These are quintessential and basic steps related to communicating information about and sending a piece of mail. Second, the Court is troubled because the claims in the SMS patent continually reference generic hardware and software. *See, e.g.*, ‘268 Patent at Col. 6:29-31) (“at least a portion of the mail verification data is sent to the reception device”); *see id.* at

⁴ Plaintiff also argues that both the United States Patent and Trademark Office (“USPTO”) and the United States Postal Service has recognized the patents’ inventive concepts. *Id.* at 19-20. The Court has reviewed and considered the prosecution history presented by Plaintiffs in its exhibits, including the dialogue at the BPAI hearing. With respect to the United States Postal Service’s adoption of the Intelligent Mail Barcode, the Court agrees with Defendant that it has “no bearing on the patentability of the Secured Mail Patents.” Reply at 11 n.4. “[T]hird-party usage of a concept is not evidence of patentability of that concept.” *Id.*

Col. 8:65-67 (“at least one *mail verification device* adapted to communicating with at least one *reception device* via a network”) (emphasis added), ‘093 Patent at Col. 1:22-26 (“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 the mail identification data over a wide area network, such as the Internet, in order to receive mail verification data.”). To the contrary, as Defendant notes, the SMS patents “stress that the invention can be performed using all types of well-known hardware, such as personal computers, set top boxes, PDAs, mobile phones, land-line phones, televisions, bar code readers, keyboards, RFID readers, smart card readers, IC readers, printers and other data storage devices.” Mot. at 18 (citing ‘268 Patent at Col. 3:25-30; *id.* at Col. 4:64-67; *id.* at Col. 5:13-15); *see also* ‘093 Patent at Col. 5:8-14 (“It should be appreciated that affixing 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 ...). “Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of ‘additional feature[e] that provides any ‘practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself.” *Alice*, 134 S. Ct. at 2358 (quoting *Mayo*, 132 S. Ct. at 1297). “The claims’ invocation of [a network such as] the Internet also adds no inventive concept.” *Ultramercial*, 772 F.3d at 716. Similarly, claims pertaining to storing, receiving data, and

providing that data via a network, *see, e.g.*, ‘268 Patent at Col. 6:27-34, are simply “routine and generic processing and storing capability[y] of computers generally.” *Affinity Labs of Texas, LLC v. DirecTV, LLC*, 2015 WL 3764356, at *21 (W.D. Tex. July 7, 2015).

2. Sender-Generated Barcode

A closer examination of the claim limitations support a finding of patent ineligibility. First, with respect to the IMb patents, the key claim is claim 1 of the ‘268 patent. As noted above, Plaintiff argues that “[o]ne of the multiple important inventive concepts in the IMb Patents is the *sender-generated barcode*.” Opp’n at 15. In the Court’s view, this is the core Step Two issue in this case. Plaintiff contends the SMS patents are inventive because “the sender can actually generate, or create, the unique identifier” that is attached to the piece of mail. Opp’n at 16. More specifically, Plaintiff describes the creation of the sender-generated barcode as follows: “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.” *Id.* at 15; ‘268 at Col. 6:21-26.⁵ Put simply, according to Plaintiff, the relevant IMb patents claims are inventive because a sender of a piece of mail can generate a unique barcode (or other

⁵ The Court notes that claims 18 and 33 of the ‘268 patent, and claims 1, 7, 11, 12, and 21, 30 of ‘860 patent also refer to either a “single set of encoded data” or a “single set of mail ID data.” Claims 5, 6, 9, 18, 20, 21, 28, 29, 33, and 39 of the ‘268 patent reference the “unique identifier.” The ‘032 patent and ‘787 patent use the term “single barcode.”

“mail identification data”) and then attach that barcode or mail ID data to a piece of mail.

The Court does not find this sender-generated barcode to be sufficiently inventive for several reasons. For one, the SMS patents simply rely on existing, well-known, standard technology. Plaintiff argues that “a [sender-based] system was novel in 2001.” Opp’n at 4, but that is not the relevant inquiry at Step Two. Rather, the key question is whether the *underlying* “technology described in the patents [was] well-known at the time of filing or simply involve[ed] performance of ‘well-understood, routine, and conventional activities commonly used in the industry.’” *Modern Telecom Sys. v. Earthlink, Inc.*, 2015 WL 1239992, at *9 (quoting *Content Extraction*, 776 F.3d at 1348). Indeed, Plaintiff does not argue the use of barcodes and other unique identifiers on pieces of mail is new. Mot. at 19 (“Using a computer to generate a barcode is merely conventional pre-solution activity and is not even arguably inventive.”); Reply at 5-6 (“SMS does not contend (nor could it contend) that the claims teach an inventive method to create the barcode or an inventive apparatus for doing so.”); see *Content Extraction*, 776 F.3d at 1348 (“[‘Patentee] conceded at oral argument that the use of a scanner or other digitized device to extra data from a document was well-known at the time of filing, as well as the ability of computers to translate the shapes on a physical page into typeface characters.”). Employing a barcode to electronically communicate data is an abstract idea that cannot be saved by narrowing the application to postal mail or personalizing the barcode for the recipient of the mail piece. In fact, the application is not even in-

ventive in the postal context as the broad idea of communicating data through barcodes is used ubiquitously through postal tracking and the sending of electronic mail delivery receipts.

Plaintiff's argument that this generic technology was not used in this particular field until 2001, *see* Opp'n at 4, therefore is unavailing. Indeed, as the *Ultramercial* held, "That some of the eleven steps were not previously employed in the art is not enough—standing alone—to confer patent eligibility upon the claims at issue." 772 F.2d at 716. Put differently, whether it was unconventional for senders – as opposed to mail carriers – to generate barcodes or other "mail identification data" and affix those to pieces of mail may be relevant to a novelty analysis under 35 U.S.C. § 102; but it does not resolve the question currently before the Court. *See Bilski*, 561 U.S. 593 at 610-11 ("[T]he fact that a company may be the first to successfully apply an abstract idea within a new technology context does not transform the abstract idea into something tangible and patentable.").

Rather, the key inquiry is whether or not the claimed limitations provides an inventive concept. To this end, Plaintiff argues the development of a unique, sender-generated identifier *is* the critical invention. The relevant claim from the '268 patent reads, "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." *See also* Opp'n at 16 ("[I]n one embodiment of the invention, the claims concatenate

both sender data, recipient data, and shipping data onto the sender-generated identifier to create a truly unique identification number ...”).

The Court does not find this claim to be inventive. The creation of a unique identifier by concatenating – or combining – four pieces of data is not sufficiently inventive. The *Digitech* court considered a similar issue in invalidating a “method for creating a device profile within a digital image processing system.” *Digitech*, 758 F.3d at 1347. In affirming the district court’s decision to invalidate the patent, the court wrote,

The above claim recites a process of taking two data sets and combining them into a single data set, the device profile. The data sets are generated by taking existing information ... and organizing this information into a new form. The above claim thus recites an ineligible abstract process of gathering and combining data that does not require input from a physical device. As discussed above, the two data sets and the resulting device profile are ineligible subject matter. Without additional limitations, a process that employs mathematical algorithms to generate additional information is not patent eligible.

Id. at 1351. The same is true here. Accordingly, the Court does not deem that the barcode (or other mail identification data) generated by the sender, as opposed to a mail carrier, to be sufficiently inventive.

But *even if* the sender-generated barcode (or other mail identification data) was a sufficiently inventive concept, the SMS patents suffer from an additional flaw; the SMS patents lack specificity in de-

scribing the supposedly inventive concepts. As Defendant puts it, the SMS patents do not “disclose *how* the sender generates the information.” Reply at 5-6; *see id.* at 2 (“Assigning the originator of a communication, however, is an abstract concept, (as SMS appears to concede), the SMS patents do not describe or claim how this information is generated.”). In this case, the ‘268 patent does not describe how the specific process or method for creating the sender-generated barcode (or other mail ID data). In other words, claim 1 of the ‘268 patent instead refers to routine “steps at ‘a high level of generality, which is insufficient to supply an inventive concept.”” *Broadband iTV, Inc. v. Hawaiian Telecom, Inc.*, Civ. No. 14-00169 ACK-RLP, 2015 WL 5769221, at *11 (D. Haw. Sept. 29, 2015) (quoting *Ultramercial*, 772 F.3d at 716); *see also Mkt. Track, LLC v. Efficient Collaborative Retail Mktg., LLC*, No. 14 C 4957, 2015 WL 3637740, at *8 (N.D. Ill. June 11, 2015); *see also id.* (“Notably, the ‘083 Patent does not disclose any technical description of *how* the steps in the process takes place.”). And contrary to Plaintiff’s suggestion, *see* Opp’n at 21, the claims at issue are not “rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks.” *DDR*, 773 F.3d at 1257. Therefore, the Court concludes that a sender-generated barcode does not add “significantly more” to the abstract ideas of gathering and combining data, and to communicating information about a piece of mail by use of a marking.⁶

⁶ As noted earlier, Plaintiff did not offer an alternative to Defendant’s characterization of the abstract idea in this case. The Court recognizes that an alternative formulation of the abstract idea may very well have

3. Bi-Directional Communication Line

Separately, Plaintiff argues the asserted claims are inventive because “this system and method can also be used to open a bi-directional communication

been “the concept of verifying transaction information.” *Card Verification Solutions, LLC v. Citigroup Inc.*, 13 C 6339, 2014 WL 4922524, at *4 (N.D. Ill. Sept. 29, 2014); *see also Morsa v. Facebook, Inc.*, 77 F. Supp. 3d 1007, 1014 (recognizing that claims may be directed to “two abstract ideas”). Plaintiff did not formulate the abstract idea in this way in its Opposition. But even if it had and the Court analyzed the SMS patents using this abstract idea, the claims at issue still lack an inventive concept for the reasons discussed. Unlike the *Card Verification* case, “there is no fundamental alteration” to the data in this case. *Netflix*, 2015 WL 4345069, at *13. The claims at issue do not provide a technical description but instead consistently refer to routine “steps at ‘a high level of generality, which is insufficient to supply an inventive concept.’” *Broadband*, 2015 WL 5769221, at *11 (quoting *Ultramercial*, 772 F.3d at 716). In many respects, the instant case is similar to *MyMedicalRecords, Inc. v. Walgreen Co.*, Nos. 2:13-006310ODW (SHx), 2:13-cv-02538-ODW (SHx), 2:13-cv-07285-ODW (SHx), 2:13-cv-03560-ODW (SHx), (C.D. Cal. Dec. 23, 2014). In that case, the court wrote,

“Claim 8 does not contain inventive concepts that make it patent-eligible. Claim 8 recites a method for providing a user with the ability to access and collect personal health records in a secure and private manner by: (1) associating access information with the user to access a server storing files; (2) providing a user interface; (3) receiving files at the server from a health care provider; (4) receiving requests through the user interface; (5) sending files; and (6) independently maintaining files on the server. All six of these concepts are routine, conventional functions of a computer and server and therefore broadly and generically claim the use of a computer and Internet to perform the abstract purpose of the asserted claims.” *Id.* at *3.

Similarly here, the claims at issue here rely on routine and conventional technology. Thus, even if Plaintiff had presented an alternate formulation of the abstract idea, the claims at issue would still fail at Step Two of the *Mayo* test.

line between a recipient and a sender of a mail piece, thereby allowing the exchange of mail related information, either from the sender to the recipient (for example, providing assembly instruction or warranty information) or from the recipient to the sender (for example, acknowledging receipt of the mail object).” Opp’n at 4. In support of this argument, Plaintiff references claims from the Personalized QR and pURL patents. Plaintiff focuses on claim 1 of the ‘002 patent – one of the pURL patents – which requires a sender-based system “that is configured to send (for example, via a sender’s web page) data identifying the recipient of the mail piece, and data corresponding to the content of the mail piece.” *Id.* at 18; *see* ‘002 Patent at Col. 6:35-54. Plaintiff argues the patent is inventive because involves “a personalized network address” that is “associated with said recipient” and results in sending the foregoing data to the recipient via “a sender’s webpage.” *Id.*⁷ Plaintiff adds that “UW has failed to show that a pURL was a conventional way of communicating mail information in 2001, before the advent of smart phones. That is because it was not.” Opp’n at 18.

The Court finds these claims are directed to the abstract idea of communicating information about a mailpiece by use of a marking; and there is no indication that Plaintiff has done more than used industry-standard technology to communicate this information. Indeed, in the “Background of the Invention” section in both the Personalized QR and pURL pa-

⁷ The Court notes that claims 3, 12, and 22 of the ‘093 patent, claims 1, 11, 20, 22, and 29 of the ‘860, claim 17 of the ‘269 patent, claim 1 and 9 make reference to either “personalized network location” or “personalized data.”

tents, it reads, “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 increases the size of the mail object.” *See, e.g.*, ‘093 Patent at Col. 1:48-53. As this description acknowledges, it is commonplace for senders to provide assembly instructions or warranty information and for recipients to acknowledge receipt of mail. The mere fact that the patents allow senders to convey this information electronically is not inventive. As Defendant correctly argues, “claiming the improved speed or efficiency inherent with the applying the abstract idea on a computer” does not amount to an inventive concept. Mot. at 12; *Bancorp Servs., LLC*, 687 F.3d at 1278 (“[T]he fact that the required calculations could be performed more efficiently via a computer does not materially alter the patent eligibility of the claimed subject matter.”); *see also CLS Bank, Int’l v. Alice Corp.*, 717 F.3d 1269, 1286 (Fed. Cir. 2013) (“[S]imply appending generic computer functionality to lend speed or efficiency to the performance of an otherwise abstract concept does not meaningfully limit claim scope for the purpose of patent eligibility.”). Plaintiff is not arguing that it invented or improved the underlying technology associated with the “personalized network address” that is “associated with said recipient” and affixed to a mailpiece; rather, Plaintiff’s core contention is that it was the first to include affix this information on pieces of mail. But just as above, Plaintiff’s argument that standard technology as it existed in 2002 was novel

and unconventional does not persuade the Court that any of the claims add an inventive concept.

At bottom, the claims Plaintiff highlights simply encompass standard uses of technology. For instance, the exchange of information between sender and recipient – what Plaintiff refers to as a “bi-directional communication line” – is simply another way of saying transmission of information over a network. This is not inventive. *See buySafe*, 765 F.3d at 1355 (“That a computer receives and sends the information over a network—with no further specification—is not even arguable inventive.”). Further, Plaintiff “does not identify any way in which the claims ‘purport to improve the functioning of the computer itself’ or ‘effect an improvement in any other technology or technical field.’” *IPLearn-Focus*, 2015 WL 4192092, at *6 (quoting *Alice*, 134 S. Ct. at 2359). As described by Plaintiff itself in a letter to Defendant, the IMb patents cover a “process of affixing, storing, receiving, and providing [data].”⁸ Patents that cover similar processes have been ruled patent ineligible. *See Content Extraction*, 776 F.3d at 1343 (“The concept of data collection, recognition, and storage is undisputedly well-known.”); *see id.* at 1349 (“[N]one of CET [plaintiff’s] claims amount to ‘significantly more’ than the abstract idea of extracting and storing data from hard copy documents using generic scanning and processing technology.”).

4. Additional Claims & Considerations

⁸ Plaintiff similarly described the Personalized QR patents as the “process of generating, affixing, submitting, receiving, and providing [data], and the pURL patents as a “process of affixing, submitting, receiving, and providing [data].”

Plaintiff points to over 100 additional claims and boldly claims, with little analysis, that those “claims include features that either add to patentability or are themselves patentable.” Opp’n at 9-10, the Court finds these remaining claims add only slight limitations that do not alter the conclusions reached above. Plaintiff broadly groups these additional claims into six categories – those that further (1) define the sender-generated mail ID data; (2) define a second set of mail ID data and how it is used; (3) define the mail data, which is personalized for the recipient, and how it is used; (4) define the electronic data – data resulting from the personalized mail data – and how it is provided; (5) define the reception device as a cellular telephone, prior to the advent of smart phones; and (6) define a second set of electronic data and how it used. *Id.* at 10. As noted above, in the Court’s view, “[n]one of the remaining asserted dependent or independent claims differ substantially” from the claims analyzed above. *See Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1378 (Fed. Cir. 2015); *see also CMG Fin. Servs.*, 50 F. Supp. 3d at 1314 (citation omitted) (“Comparing the language of the systems claims with that of the method claims, it is clear that these are functionally identical ... Thus, they must be treated as equivalent for purposes of the § 101 analysis.”).

Still, the Court proceeds to consider the claims identified by Plaintiff in his Opposition. Plaintiff specifically points to claims 9 and 16 of the ‘002 patent and claims 11 and 21 of the ‘860 patent, which provide a “sender-based system and mail ID data that is personalized for the recipient and used to send at least content data to the recipient via a

sender's web page;" claim 1 of the '860 patent which provides a "sender-based system and mail ID data that includes a personalized network address associated with the recipient and used to send content data to the recipient;" claims 1, 10, and 17 of the '629 patent and claims 1, 10, and 20 of the '093 patent that provide a "sender-based system and mail ID data that is personalized for the recipient and used to send at least content data to recipient." Opp'n at 18. A closer look at these claims, however, reveals they use very similar language as the claims discussed above, and they suffer from the same defects. For instance, claim 9 of the '002 patent describes, "[a] system for providing electronic data to a recipient of a mail object." '002 Patent at Col. 7:10-11; claim 1 of the '860 patent describes, "[a] method for providing electronic data to a recipient of a mail object." '860 Patent at Col. 6:34-35; and claim 10 of the '093 describes "[a] system for providing electronic data to a recipient of a mail object." Variations between these claims are trivial, and they simply incorporate the same purportedly inventive concepts discussed above.

Therefore, the Court does not find anything inventive about these additional claims. Including a "personalized" marker on a piece of mail is not inventive; differences in the content of the information communicated (i.e., the type of data) or the type of device involved are not sufficiently inventive to confer patent eligibility; and fundamentally, Plaintiff has not identified in any way in which these claims "effect an improvement in any other technology or technical field," *IPLearn-Focus*, 2015 WL 4192092, at *6 (quoting *Alice*, 134 S. Ct. at 2359). Again, these

claims describe conventional communication that takes place between the sender and a recipient of a piece of mail and rely on routine and conventional technology. Additionally, the Court notes that the claims' general language regarding authentication or encoding of data are not sufficiently inventive. *See, e.g.*, '268 Patent at Col. 7:20 ("The method of claim 1, where said step of providing mail verification data further comprises providing at least authenticating data to said at least one reception device."); *see also Kinglite Holdings, Inc. v. Micro-Star Int'l Co.*, No. 2:14-cv-03009 (C.D. Cal. Oct. 16, 2015) at 14 ("The Court agrees with Defendants' characterization that these steps simply 'implicate the concept of authentication or verification of a request.' As seen in *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370-73 (Fed. Cir. 2011), claims reciting a method of authenticating for security purposes are directed to an abstract idea."). As Defendant notes, "the patent provides no explanation whatsoever of *how* the step of authentication of the mail ID is accomplished." Mot. at 21. Rather, as with the claims discussed above, the claims consistently refer to routine "steps at 'a high level of generality, which is insufficient to supply an inventive concept.'" *Broadband*, 2015 WL 5769221, at *11 (quoting *Ultramar*, 772 F.3d at 716). Thus, the Court does not find the additional independent or dependent claims are sufficiently inventive.

The Court's conclusion that the asserted claims fail is further confirmed by the application of the machine-or-transformation test. While the machine-or-transformation test is not dispositive when conducting at § 101 analysis, it serves as a "useful and

important clue.” *Ultramercial*, 772 F.3d at 716 (quoting *Bilski*, 561 U.S. at 604). Here, as in *Ultramercial*, none of the asserted claims are “tied to any particular novel machine.” *Id.* As described above, the claims stress that the invention can be performed using a number of well-known devices. Any reference to networks, such as the Internet, are likewise insufficient to tie the claim to a particular novel machine. See *CyberSource Corp*, 654 F.3d at 1370 (explaining that the recitation of the Internet as a source of data does not tie a claim to a particular machine). The asserted claims likely fail to satisfy the transformation prong of the machine-or-transformation test. The system and methods claimed refer generally to the combining of data, or the transmission of data between a sender and recipient of a piece of mail. This does not qualify as transformation within the meaning of the test. See *id.* at 1375 (“[T]he mere manipulation or reorganization of data ... does not satisfy the transformation prong.”). Plaintiff did not explicitly reference the machine-or-transformation test in its Opposition; and Plaintiff has failed to convincingly argue the concatenation of data qualifies as a “fundamental alteration to the information itself.” *Netflix*, 2015 WL 4345069, at *13 (internal quotation marks omitted). And as mentioned above, the SMS patents lack the requisite technical description of how the sender-generated barcode operates. Thus, the asserted claims do not transform any article into a different state or thing. While a claim’s satisfaction of the machine-or-transformation test is not dispositive, it underscores why the claims do not supply an inventive concept.

Finally, the Court’s conclusion is buttressed by what the Supreme Court characterized as the “preemption concern that undergirds our § 101 jurisprudence.” *See Alice*, 134 S. Ct. at 2358. The claims in the SMS patent do not meaningfully limit the abstract idea of communicating information about a mailpiece by use of a marking; as a result, the Court has serious concerns that the SMS patents could significantly foreclose future innovation. In contrast to *Intellectual Ventures*, the SMS patents do not disclose a “specific method” of creating the mail identification data, communicating the data, authenticating the data, or receiving the data. *See Netflix*, 2015 WL 4345069, at *17. “Neither the claims themselves nor [Plaintiff’s] brief contain any meaningful disclosure of *how*” these methods actually take place, *Netflix*, 2015 WL 4345069, at *17; rather, the SMS patents simply reference the claimed methods in general terms. The Court finds that the claims pertain only to senders of mail is not meaningful limitation. Because the asserted claims are not limited in any meaningful way, it raises significant concerns that the claims will preempt a large number of ways of communicating information about a piece of mail by use of a marking. This factor further counsels against finding the asserted claims patent eligible.

In sum, the asserted claims, viewed individually or in combination, do not meaningfully limit the abstract idea of communicating information about a mailpiece by use of marking. As a result, the Court finds each of the asserted claims unpatentable under § 101.

IV. Disposition

For the reasons set forth above, the Court finds the '032 patent, the '268 patent, the '787 patent, the '629 patent, the '093 patent, the '860 patent, and the '002 patents invalid under § 101. Accordingly, Defendant's Motion is GRANTED.

The Clerk shall serve this Minute Order on the parties.

Initials of Deputy Clerk

**FINAL ORDER ON CLAIM CONSTRUCTION
(APRIL 8, 2014)**

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SECURED MAIL SOLUTIONS, LLC,
Plaintiff,

v.

ADVANCED IMAGE DIRECT LLC, ET AL.,
DefendantS.

Case No. SACV 12-01090 DOC (RNBx)
Re: Dkt. No. 195

Before: David O. CARTER
United States District Court Judge

Before the Court are Plaintiff's Motion for Summary Judgment of Infringement (Dkt. 139) and Motion for Summary Judgment of Validity (Dkt. 138) and Defendants' Motion for Summary Judgment of Non-infringement (Dkt. 143). The parties simultaneously briefed claim construction issues. The Court considers only the claim construction issues at this time, and will issue a separate ruling on the motions for summary judgment on infringement and validity.

I. Background

This lawsuit addresses software tools designed to aid in large-scale commercial mailings. Defendants Envelopes Unlimited (“EU”) and Advanced Image Direct (“AID”) produce and send mailings on behalf of their clients. Clients give AID and EU the contents and design of the mailing the client wishes to send and the mailing information for where the client wants the mailings sent. EU and AID print and send the mailings using specialized software and processes that qualify for specific discounts from the United States Postal Service (“USPS”).

Plaintiff Secured Mail Solutions (“SMS”) claims that Defendants are infringing on its method and system patents that set out a way of assigning specific identifying information to pieces of mail and then using post office data to verify that information. Some of the allegedly infringing processes are performed by a third party, GrayHair, which is not named in this lawsuit. EU and AID use GrayHair’s software (a primary program called GHSelect and an add-on called SelectTrak) to assign identifying information to track mailings. SMS claims that EU and AID are liable for infringement performed in part by GrayHair.

The parties briefed and argued their *Markman* and dispositive motion issues. This order constitutes the Court’s final ruling on claim construction.

a. Patents at Issue

This case centers on a series of patents that issued from a provisional application filed on October 16, 2011. See Fitzsimmons Decl. Ex. A-1. Three are relevant to this litigation: U.S. Patent No. 7,814,032 (the “032 Patent”), U.S. Patent No. 7,818, 268 (the

“268 Patent”), and U.S. Patent No. 8,073,787 (the “787 Patent”). Only claims in the ‘268 and ‘787 Patents remain at issue in this lawsuit. These patents are similar and share much overlapping language. Both address methods of using encoded data on the outside of mail pieces to verify or authenticate those mail pieces.

The inventor and president of SMS, Todd Fitzsimmons, developed the idea for this series of patents after the events of September 11, 2011. Fitzsimmons Decl. ¶ 5. Mr. Fitzsimmons imagined that the patented system could protect mail recipients from possible anthrax or explosive attacks by mail because the system would permit recipients to verify the source of the package before opening it. *Id.* at ¶¶ 5-8.

b. Claims at Issue

Plaintiff alleges that Defendants are infringing the following claims in the ‘268 Patent:

Claim 1

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 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.

See '268 Patent 6:18-37.

Claim 1 Dependent Claims

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.

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.

See '268 Patent 6:49-55, 7:1-7.

Claim 33

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 communicating 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

Providing mail verification data via said network if at least said authenticating portion of said mail identification data corre-

sponds to said verifying portion of said mail identification data.

See '268 Patent 8:62-9:19.

Claim 33 dependent Claims

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.

See '268 Patent 9:38-43.

Plaintiff alleges that Defendants infringe the following claims in the '787 Patent:

Claim 1

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:

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.

See '787 Patent 6:28—6:58.

Claim 30

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 20 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.

See '787 Patent 9:14-36.

Claim 30 Dependent Claims

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.

See '787 Patent 9:40-42.

II. Legal Standard

Patent infringement analysis involves two steps: (1) an interpretation of the asserted claims, and (2) a comparison of the claims to the accused device. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995) (*en banc*), *aff'd*, 517 U.S. 370, 116 S. Ct.1384 (1996). Claim interpretation is a matter of law, *id.* at 979, and is thus amenable to summary judgment, even though the analysis involves both issues of law and questions of fact. *Phonometrics Inc. v. N. Telecom Inc.*, 133 F.3d 1459, 1463-64 (Fed. Cir. 1998). Many courts, however, have chosen to hold a claim interpretation hearing, or *Markman* hearing, to facilitate the claim interpretation process. *See, e.g., Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 93 F.3d 1572, 1577 (Fed. Cir. 1996).

Claim interpretation begins with the language of the claims. *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1324 (Fed. Cir. 2002). Terms in the claims are generally given the ordinary and customer meaning they would have to a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*). However, the terms must be read in the context of the entire patent. *Id.* at 1314. In interpreting the claims, the court focuses primarily on the intrinsic evidence of record, including the claims themselves, the specification, and if in evidence, the prosecution history. *Id.* at 1312-17.

Among the intrinsic evidence, the specification is always highly relevant to the claim construction analysis—it is the single best guide to the meaning

of a disputed term, and is usually dispositive. *Id.* at 1315 (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). “The specification is, thus, the primary basis for construing the claims.” *Id.* (quoting *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985)). In addition to the specification, the court will also consider the prosecution history, consisting of “the complete record” of the patent. *Id.* at 1317. However, because the prosecution history often lacks the clarity of the specification, it is less useful for claim construction purposes. *Id.*

While the court may also consider extrinsic evidence, including expert testimony, dictionaries, and learned treatises, as the Federal Circuit has recently made clear, such evidence is generally viewed as less reliable than intrinsic evidence. *Phillips*, 415 F.3d at 1317-18. Therefore, the court must use its discretion in admitting and weighing extrinsic evidence, keeping in mind its inherent flaws. *Id.* at 1319.

III. Claim Construction

The parties request construction of four terms: 1) “sender,” and related terms; 2) “recipient” and related terms; 3) “mail verification data” and “verifying data”; and 4) “mail verification device.” The Court addresses each in turn.

a. “Sender,” “Sender Data,” and “Sender Portion”

At the outset, the Court addresses the construction of “sender data,” as it is directly defined in each Patent’s specifications. The parties agree that “sender data” is indistinguishable from “sender portion” or

“sender information.” HT2 at 43. “Sender data” is defined in the ‘268 Patent’s specification as “indicating who sent the mail object.” ‘268 Patent 2:32-33; 4:54. In a hearing held before the Board of Patent Appeals and Interferences (“BPAI”) on the ‘268 Patent, the inventor told the Board that “sender data” is defined as “data that can be used to identify the sender.” See Fitzsimmons Decl. Ex. A-4 at 527. At the final *Markman* hearing, the parties seemed to largely agree on a construction that of “information indicating who the sender is.” HT3 at 28. This seems to the Court indistinguishable from the specification definition. The Court therefore adopts the definition provided in the specification, as it is part of the intrinsic evidence and does not appear functionally distinct from the definition given to the BPAI. This also serves as the construction for “sender portion” and “sender information,” per the parties’ agreement. The Court therefore turns to the parties’ greater point of dispute: “sender.”

“Sender” is a central term in all of the contested claims. Plaintiff first argued that the Court should construe “Sender” as “any person or entity that is involved in the sending of a mail object to a recipient via a mail carrier.” Opp’n at 4. Defendants countered that “sender” is more properly construed with its common dictionary definition as a “person or entity that conveys or causes to be conveyed by an agent, the mail piece.” See Ds Opp’n to PMSJ at 8. SMS later presented a first alternative construction: “Any person or entity that is involved in the preparation of the mail object for the mail carrier or identified on

the mail object as a sender of the mail object.” HT2¹ at 24. Defendants preferred this construction, but argued that “sender” should be narrowed to an individual or entity who initiates the content or otherwise commissions the mailing, or an entity that actually packages or handles the mail object itself. See HT2 at 36-37. At the final hearing, Plaintiff again revised its position to argue that the sender is “the entity that assigns the unique identifier.” HT3 at 10.

The Court concludes that the most accurate construction of “sender,” and the only definition identified in the claims or the specifications of the patents, should simply be derived from the “sender data” definition: “who sent the mail object.” ‘268 Patent 2:32-33; 4:54. If the inventor describes “sender data” as “data that can be used to identify the sender,” *see* Fitzsimmons Decl. Ex. A-4 at 527, and the specification identifies the same data as “indicating who sent the mail object,” the only logical inference is that the “sender” is the person or entity “who sent the mail object.” “Sent” should have its common meaning, rather than any specialized definition. “To send” is generally defined as: “To cause to be conveyed by an intermediary to a destination <send books to California by train>,” or “To dispatch, as by a communications medium <send a letter> <sent a telegram>,” *Merriam Webster New College Dictionary II* 1005 (1995), or, similarly, “To cause to go or be taken to a particular destination, arrange for the delivery of, esp. by mail,” *Oxford American Dictionary* 1589 (3d

¹ The Court held multiple hearings on this matter, and delineates between the transcripts by using a numeral following “HT.” References to the transcripts from the first hearing are therefore cited with “HT,” from the second hearing with “HT2,” and so forth.

ed. 2010). This is consistent with the clear direction in the claims and the patents' specifications that the sender should be directly associated with the physical mail object in some way.

In reaching this construction, the Court turns first to the claim terms. *Teleflex*, 299 F.3d at 1324. The term is not expressly defined anywhere in the claims. The claim language of the '268 and '787 Patents, however, make it clear that the sender assigns the unique identifier that is always included in the mail identification data. *See* '268 Patent 6:25; '787 Patent 5:40. The '787 Patent further states that this value assigned by the sender can be used to identify the sender of the mail object, suggesting that the sender should be somehow associated with the source of the mail object itself. *See* '787 Patent 6:35-60 ("at least a portion of [the mail identification data] ... can be used by said mail carrier to identify said sender of said mail object."). These two aspects of the "sender" ring true through the intrinsic evidence, and support using the construction above.

The specifications of the '268 and '787 Patents also support using the above construction and the common definition of "to send." First, each specification suggests a definition of "sender" that requires the sender to be somehow in contact with the mail piece or the source of the mail piece in some way. The specifications define "sender data" as "indicating who sent the mail object," which suggests that the "sender" is the person or entity "who sent the mail object." *See* '268 Patent 4:45; '787 Patent 4:62. There is nothing in either the specifications or claims suggesting that "send" or "sent" means anything other than its plain and ordinary meaning, which further

suggests that a sender is one who is directly involved in placing the mail object in the mail stream or directing its placement in the mail stream.

Second, both specifications describe two “problems” that the inventions are designed to mitigate. The first problem is security, and the claimed invention is designed to provide a method of screening mail to prevent exposing recipients to hazardous substances from unknown sources or other unwanted mail. *See* ‘268 Patent 1:30-40; ‘787 Patent 1:32-45. The second problem is that manual delivery “is limited to a one-way production of a finite set of information,” creating problems when “the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.).” ‘268 Patent 1:43-49; ‘787 Patent 1:46-50. The method also allows information that would otherwise have been mailed in hard copy to be sent electronically to reduce costs and the size of the mail object. *See* ‘268 Patent 1:50-55; ‘787 Patent 1:50-59. These purposes are only served if the “sender” is a person or entity who either directed the content of the mailing or was part of the mailing of the physical mail object. Screening packages is only effective if the “sender data” gives the opener some knowledge of where or who the package came from, or what might be in it. Similarly, a person or entity invested in the contents of the mail object or its actual shipment would be much more likely to be concerned about providing product information or reducing shipping costs.

The extrinsic evidence from the prosecution history also supports construing “sender” to require some connection to an entity or person who either

directed the content of the mailing or otherwise handled the mail piece. In the BPAI hearing, the inventor made clear that the defining feature of the invention is the ability to use information from the mail object's sender to verify or identify the sender, or the source, of that mail object. The inventor told the Board that "sender data" is defined as "data that can be used to identify the sender." *See* Fitzsimmons Decl. Ex. A-4 at 527. The inventor further explained that the application addressed a "system and method of verifying a mail object" by using data including "a unique identifier that is then *used to identify, or verify, that the mail object came from an identifiable entity.*" Fitzsimmons Decl. Ex. A-4 at 517 (emphasis added). The inventor repeated this sentiment again when emphasizing that part of the "claimed invention" is the use of the encoded data "to then verify that the mail object was sent by an identifiable entity." Fitzsimmons Decl. Ex. A-4 at 523.

The Court was initially concerned that there may be some dispute over whether the term "sender" contemplated multiple senders in any given scenario, i.e., that for purposes of the patented method, there might be an initial party providing the contents of the mailings, a separate party packaging the mail pieces, another party transporting the mail pieces to the post office, and so forth, all of whom could be "senders." At first, the parties agreed that there may be more than one "sender" for any given mail piece. At the final hearing, however, Plaintiff changed its claim construction theory and adopted the position that there could be only one sender for purposes of the method, defined as the individual or entity that assigned the unique identifier. Plaintiff argues that

this contrition is the most accurate and the fact mandated by the claim terms because the unique identifier is, by definition, assigned by the sender. *See* ‘268 Patent 6:25. Defendants do not dispute that there could be only one sender, but argue that this construction is redundant.

The Court agrees with the parties that one entity or person serves as the same “sender” for all purposes under the ‘268 and ‘787 Patents, although the definition of “sender” allows for a number of types of entities to fulfill that function in any given scenario. The Court disagrees with Plaintiff’s proposed construction, however, because it is circular and unsupported by the claims. First, the only definition of sender comes from the definition of “sender data,” defined as data “indicating who sent the mail package.” This entity identified in the “sender data” must also assign the unique identifier for a method to be covered by the patented claims, but the “sender data” is defined by conveying of the mail object, not, indicating who assigned the “unique identifier.” Second, there is simply no suggestion in the claims or specifications that anyone who assigns a unique identifier is a sender for purposes of the patent. All other references to the sender identify it as the source of the mail object or mail contents, not simply the source of the identifier. Indeed, the purposes described in the patents’ specifications would not be furthered if the sender were simply the entity that assigned the identifier, but need have no connection to the contents or mailing of the actual mail piece. This would neither allow the recipient to confirm the source of the package for safety reasons, nor help an entity avoid additional shipping challenges. The in-

ventor could have made this distinction vividly clear in the claims and specifications, but chose not to.

It is certainly true that the unique identifier must be assigned by the sender, and that this is a crucial piece of the patented invention. The inventor made it clear at the BPAI hearing that this was a defining aspect of the patent. The inventor specifically distinguished the invention based on this feature, explaining that “the prior art ... does not teach a situation where a sender provides a non-unique value and you have to concatenate data onto that in order to render a unique value.” Fitzsimmons Decl. Ex. A-4 at 525. The inventor stated that one application of the invention was to allow a sender to generate identifying information that was still unique enough to provide tracking, explaining that “the application solves the problem of how do you allow the sender to generate a unique identifier, and they also ensure that that identifier is truly unique enough to track or identify the mail object.” Fitzsimmons Decl. Ex. A-4 at 517-518. Furthermore, in response to the BPAI’s question, “If I understand what you’re saying, is that the distinctive aspect of your invention is this string, single set of encoded data, and that it includes a unique identifier, sender data, recipient data, and shipping method data?”, the inventor responded, “Correct. Where the unique identifier is generated by the sender, correct.” Fitzsimmons Decl. Ex. A-4 at 527; *see also* Fitzsimmons Decl. A-4 at 528 (“And the unique identifier is assigned by the sender, or, in the specification, it talks about being generated by the sender.”). But it does not follow that any assigned unique identifier is assigned by the sender. Rather, there is some pool of entities involved in conveying a

mail piece that meet the definition of “sender.” How those entities are identified in the encoded data will then be determined whether they are, in fact, “senders” infringing on these patents.

Plaintiff objected to Defendants’ construction on the grounds that it was inconsistent with the intrinsic evidence and is based solely on extrinsic evidence. Because the Court adopts the Defendants’ definition of “send,” although not its actual construction, the Court addresses this argument. As discussed above, the common definition of “send” is entirely supported by the intrinsic evidence. All discussions of “sender” in the claims, specification, and history show that a sender must be associated with the contents or physical mail piece involved – they must either cause a certain item to be conveyed (perhaps directing someone else to put out a specific mailing), or convey the object in some way. The definition of “sender data” supports this construction, as do the listed embodiments and the stated purposes for the patent.

The crux of the issue is: any entity that sends a mail piece in the common meaning can be a “sender” within the meaning of the claims. That sender must also be “indicated” in the “sender data.” Finally, that sender must have assigned the unique identifier in the mail ID data. Therefore, Plaintiff is correct that for the purpose of this method, the “sender” is the entity that assigns the unique identifier. However, the fact of assigning the unique identifier does not inform whether an entity can qualify as a “sender” for purposes of the patents. Instead, an entity or person who can be considered a “sender” under the patent must be “indicated” by the sender data and

must also be the person or entity “who sent the mail object.”

The Court concludes that the construing “sender” to be the “person or entity who sent the mail object” is the construction most consistent with the claim language, specifications of the patents, prosecution history, and articulated purpose of the invention.

b. Recipient Data

At the second hearing, the parties stipulated to the following construction: “information indicating who is to receive the mail object, which may include the recipient’s address or account number.” HT2 at 46. This appears to the Court to be consistent with the claims and specification. Again, the parties do not dispute that “recipient portion” and “recipient information” should have the same construction as “recipient data.”

c. “Mail Verification Data” and “Verifying Data”

The parties agree that “mail verification data” and “verifying data” should have the same construction (as distinct from the “verifying portion” of the mail identification data). HT2 at 47. Plaintiff’s final proposed construction is, “data from the sender of the mail object.” Defendants’ final proposed construction is: “data from a mail verification application provided to a reception device if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.” *See* HT2 at 50.

Based on the intrinsic evidence and prosecution history, the Court concludes that “mail verification

data” and “verifying data” are properly construed as simply “data from a mail verification application that is provided if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.” The Court declines to import limitations requiring either that the data come from the sender or be sent to the recipient.

From the claims and the specification, it is clear that mail verification data is generated when the authenticating and verifying portions of the mail ID correspond. It is also apparent that the mail verification application, which is on the mail ID device, provides the mail verification data. Mail verification data is not actually defined, however, Claim 1 of the ‘268 Patent provides that “mail verification data” is provided “by said computer” via the network “when said authenticating portion of said mail identification data corresponds with said verifying portion of said mail identification data.” ‘268 Patent 6:34-37. Claims 11 through 15 of the ‘268 Patent describe the method of Claim 1, but provide variations on the content and destination of the mail verification data. ‘268 Patent at 7:15-31.

In the “Background of the Invention” in the ‘268 Patent, the invention is described as “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.” ‘268 Patent at 1:16-19. The detailed description explains that the mail verification application is part of the mail ID device, and the mail verification application stores the verifying portion of the mail ID data, receives the authenticating portion of the mail ID data from

the reception device, and provides the mail verification data if the authenticating portion is authenticated (i.e., corresponds). *See* ‘268 Patent 3:35-42. This description is echoed in the description of another embodiment, describing the mail verification application running on the mail ID device as comparing the authenticating portion of the mail ID with the stored verifying portion. If there is correspondence, “then mail verification data is sent to the reception device.” ‘268 Patent 4:38-44. The detailed description further suggests one possible embodiment in which the mail verification data could include authenticating data, securing data (showing who secured the mail object), sender data, or recipient data. *See* ‘268 Patent 4:45-58.

There are no requirements for the content of the mail verification data. The specification provides that it may include recipient data, sender data, securing data (“including who secured the mail object”), or additional data including instructions, product data, third party advertisements, etc. *See* ‘268 Patent 2:30-35. Thus, although the claims use the term “verifying data,” the specification is clear that the actual information need not confirm anything specific about the package’s contents or sender, and need not provide any particular information about the package’s origin. Mail verification data can serve either of the two enumerated purposes of the ‘268 Patent: ensuring or verifying the package’s source or contents for safety reasons, or providing information that might otherwise have required physical mailing.

The first dispute the Court must address is whether the construction should include a destina-

tion. Defendants argue that the mail verification data must go to a reception device or a recipient. See HT2 at 57-58. This limitation seems improper, however, in light of claims 11 through 15, which designates different destinations for the mail verification data, including “at least one reception device” (claim 11), and “a recipient” (claim 13). These claims are dependent claims of Claim 1, suggesting that Claim 1 is broader than either of these two requirements. Although the preferred embodiment specify that the mail verification data should be sent to the reception device. Claim 13 contains the limitations of the verification being data sent to the recipient. Claims 11 and 13 are dependent claims to Claim 1, and so the limitation it provides cannot apply to all claims. See *Phillips*, 415 F.3d at 1315. Furthermore, the inventor removed exactly this limitation from his application during prosecution for reasons that are not explained. See Fitzsimmons Decl. Ex. A-4 at 346. It would be improper to read such a limitation back into the patent after it has been expressly removed. *Laryngeal Mask Co. Ltd. v. Ambu*, 618 F.3d 1367, 1372 (Fed. Cir. 2010).

In addition to the question whether mail verification data must go to a specific entity or location, the parties also dispute whether mail verification must come *from* a sender. Although the Court was initially inclined to agree that mail verification data could be construed to come from a sender, this construction does not actually appear supported in the claim or the specification language. The more accurate description seems to be to describe the verification data as coming from the mail verification application upon correspondence between the verifying and au-

thenticating ID portions; there is no language in the claims or specifications that would suggest the verification data comes only from the sender.

Indeed, the specification suggest that mail verification data could include information that has nothing to do with the sender. For example, the Summary of the Invention states that the mail verification data could include securing data (“indicating who secured the mail object”), and/or sender data, clearly suggesting that the “securing” and “sending” parties could be different individuals. It would make sense for securing data to come from a securing party separate from the sender, especially if the securing party confirmed the contents’ safety, inspection, or secure transport. Similarly, the Summary considers the possibility that the mail verification data may include “third party advertisements,” which appear by definition to originate not with the sender. These details also appear in the description of the preferred embodiment. *See* ‘268 4:52-58. Finally, the description of the preferred embodiment describes one embodiment in which the mail verification data includes “software-booting data adapted to boot an email application and/or a browser application,” either one of which could be used to “receive additional information from either the mail ID device, the sender of the mail object, or a third party.” *See* ‘268 Patent 5:35-41. This further suggests that the mail verification data is not exclusively in the purview of the sender.

Because there is no indication in the claims that the mail verification data comes from the sender, the only basis to associate this data with the sender appears to be through the mail ID or verification device.

es. Mail verification data is produced by the mail verification application, which resides on the mail ID device, which Plaintiff argue is controlled or operated by the sender. Leaving aside for now whether the mail ID device is so controlled, it seems unnecessary and outside the actual claims and specification to attribute any origin to the mail verification data itself. It further appears, based on the above discussion, that even if the data were generated by a device controlled by the sender, the content or data provided might be from a different entity. The Court therefore declines to read a limitation into the claims that appears unsupported in the patents. Plaintiff elaborates on this point by arguing that “the sender that generated the mail ID data is the one who can ‘verify’ or ‘authenticate’ the mail ID data.” Even if the Court were to accept this argument, it does not follow that the data produced after verification or authentication is necessarily from the sender itself. Indeed, the actual data may not “verify” or “authenticate” anything about the piece, but instead acts as a confirmation of “correspondence” that can take many forms.

The experts on each side do little to clarify this question. Dr. Lopresti opines that the term should be construed as “data from an authorized sender,” Lopresti Decl. ¶¶ 102-03, but there is nothing in the claim language or specification that explains how the Court should construe “authorized sender.” Dr. Allais opines that the “mail verification data” is “data transmitted by the Mail Identification Device.” Allais Decl. ¶¶ 43-45. Dr. Allais further opines that the “mail identification device” is “associated with a location where the mail originates.” Allais Decl. ¶¶ 26-

32. Again, this does not suggest a need to import any further limitation to the “mail verification data.”

The Court understands the common sense appeal of assuming that all verifying data will be “from” the sender in some sense. This appears to be the intent of the preferred embodiments, and makes intuitive sense. On the other hand, the inventor presented the patents as defined by the sender-generated unique identifier, which is specifically identified as such in the patent. It was possible for the inventor to also define mail verification data as being generated, assigned, or otherwise from the sender, but there is no such limitation. It also appears to the Court that there are possible embodiments for which the verifying data is not from the sender, possibly in the embodiment involving an independent security institution or a government office.

The Court is therefore inclined to construe “mail verification data” and “verifying data” as simply “data from a mail verification application that is provided if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.”

d. Mail Verification Device

The term “mail verification device” is not used in the ‘268 Patent until Claim 33, and is used again in Claim 52. No definition is provided in the specification or claims. The mail verification device appears to play the same role that the mail ID device plays in Claim 1, and this is the position Plaintiff adopts. Plaintiff argues that “mail verification device,” and thus by extension mail ID device, should be construed as a “device operated by a sender of the mail

object.” Defendants respond that the mail verification device (and thus the mail ID device) should not be construed as “sender operated.” Based on the claim language and specification, the Court concludes that the mail verification device is: “a device adapted to communicate with one or more reception devices via a network, comprised of at least a memory and a mail verification application adapted to store the verifying portion of the mail ID data, receive the authenticating portion of mail ID data, and provide mail verification data.” The Court sees no basis in the claims or specification of the ‘268 Patent for narrowing this construction further, or importing a “sender-operated” limitation.

Turning first to the claims and specification, the Court notes that “mail verification device” has no explicit definition. The fullest description is in Claim 33 of the ‘268 Patent, which provides:

33. A mail verification system for authenticating at least one mail object ... 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

... ;

receive at least an authenticating portion of said mail identification data from said at

least one reception device via said network
... ; and
provide mail verification data via said
network ...

‘268 Patent 8:62-9:19. The description and figures make clear that it is the device that hosts the mail verification application, and so is the device that receives data from the reception device to determine whether there is “correspondence.” In a colloquial sense, it is the device or computer at the front end of the process of verifying a mail object – storing a piece of data that will later be compared to data sent from the scanner or other form of reception device where the mail object arrives. This reinforces that the mail verification device and the mail ID device perform the same basic function.

The only indication Plaintiff cites for the mail ID device and the mail verification device being “sender operated” are expert opinions and statements made by the inventors during prosecution. The inventor’s statements, however, appear to discuss one possible embodiment, not all possible embodiments. *See Fitzsimmons Decl. Ex. A-4 at 402-403* (“In *one embodiment* of the present invention, a sender uses a mail ID device ...”) (“The specification further provides that a sender *can* use a mail ID device (110) or more particularly, a mail verification application (112) operating thereon ...”) (emphasis added). Defendants’ expert opines that the mail verification device “would logically be the same as the Mail Identification Device” because the mail verification application resides on the mail ID device. *See Allais Decl. ¶ 42*. Plaintiff’s expert writes that “the mail verification

device is used by a sender of the mail object,” but does not opine further. *See* Sterling Rebuttal Decl. ¶ 36.

Both experts opine more fully on the meaning of “mail identification device.” Defendants’ expert looks to the common specification and notes that the mail ID device is “associated with a location where the mail originates.” Allais Decl. ¶ 31. Plaintiff’s expert opines that the mail ID device “is described in common specification as being used by a sender of the mail object.” Sterling Rebuttal ¶ 21. Sterling further supports this position with a statement made by the inventor during the prosecution history (“a sender can use a mail ID device (110), or more particularly, a mail verification application (112) operating thereon, to generate the mail ID data (or a portion thereof).” Sterling Rebuttal Decl. ¶ 21. The inventor also stated that the mail ID device could be used to compare received data to stored data, possibly “to determine whether a mail object was sent from a secure location or an authorized (or at least identifiable) entity.” Sterling Rebuttal Decl. ¶ 21. Based on this evidence, Sterling opined that “the mail ID device is associated with a sender of the mail object, and more particularly, is used by a sender of the mail object to store, receive and compare mail ID data, or a portion thereof.” Sterling Rebuttal ¶ 22.

Although the court understands the intuitive appeal of reading a “sender-operated” limitation into the claim language, this does not seem supported by the patent itself. The references to a sender operating the mail ID device or mail verification device are not mandatory; they are rather iterations of the invention or the preferred embodiment. The claims

themselves are broader. The claims and specification in fact appear to run against a “sender operated” limitation. First, the ‘268 Patent specifically associates the unique identifier with the sender, showing that the inventor could have specified that the mail ID device or mail verification device were also specifically related to the sender. *See* ‘268 Patent 6:24-26 (“... wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object.”).

Second, there are several proposed embodiments in which the sender and the mail ID device are entirely separate, further suggesting that the mail ID device cannot be construed to *always* be sender-operated. *See* ‘268 Patent 5:29-35 (“Either one of these applications could then be used to ... 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.”); ‘268 Patent 5:35-41 (“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.”); ‘268 Patent 5:42-49 (“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 ... or manually, to allow the recipient

to communicate with the mail ID device *and/or* sender of the mail object.”) (emphasis added). Thus, because the claims and specification contain no language limiting the mail verification device or mail ID device to a sender’s control, and the specification in fact suggests embodiments in which the sender and mail ID device are contacted separately, the Court declines to read this limitation into the ‘268 Patent. This leaves open the question of how the mail verification device should in fact be construed.

From this, the Court concludes that the mail verification device is simply defined by its terms in the claims: “a device adapted to communicate with one or more reception devices via a network, comprised of at least a memory and a mail verification application adapted to store the verifying portion of the mail ID data, receive the authenticating portion of mail ID data, and provide mail verification data.” The Court sees no basis in the claims or specification of the ‘268 Patent for further describing a mail verification device or narrowing this construction.

IV. Disposition

The Court hereby adopts the foregoing claim constructions for the claims at issue. The Court will issue a separate order on the motions for summary judgment.

DATED: April 8, 2014

/s/ David O. Carter

DAVID O. CARTER
UNITED STATES DISTRICT JUDGE

**SUPPLEMENTAL STATEMENT RE:
PETITION TO MAKE SPECIAL
(SEPTEMBER 2, 2003)**

IN THE UNITED STATES PATENT
AND TRADEMARK OFFICE

Applicant: TODD E. FITZSIMMONS
Serial No. 10/271,471
Filed: October 15, 2002
Title: SYSTEM AND METHOD FOR MAIL
VERIFICATION

Sir:

In response to the Decision on Petition to Make Special (Counter Terrorism), dated June 30, 2003, please consider the following supplemental statement:

SUPPLEMENTAL STATEMENT

The Applicant respectfully requests reconsideration and review of Applicant's Petition for Special Application Status, which was filed on October 15, 2002 and made pursuant to 37 C.F.R. § 1.102(d), in view of the following statement.

Shipping hazardous materials to a particular individual (or organization) is one method of carrying out an act of terrorism. For example, shortly after

the tragic events of September 11, 2001, Anthrax was shipped to a number of government officials. These shipments were made using the United States Postal Service and were considered acts of terrorism. The present invention provides a system and method of verifying or authenticating a mail object before the mail object is opened, thus minimizing the recipient's exposure to the contents located therein.

For example, in one embodiment of the present invention (see Figure 1), mail ID data 132 (e.g., a unique alphanumeric sequence, etc.) is affixed to a mail object 130 and provided to a mail ID device 110, wherein the mail ID device 110 is adapted to store the mail ID data 132 (e.g., in a database). The mail object 130 is then manually delivered to a recipient and the mail ID data 132, as attached thereto, is provided to a reception device 120. The reception device 120 is adapted to transmit the mail ID data 132 to the mail ID device 110 (e.g., over the Internet), where it is compared to the data that was previously stored. If the data transmitted corresponds to the data previously stored (e.g., matches the data previously stored, etc.), mail verification data is transmitted to the reception device 120. The recipient is accordingly notified (e.g., through audio and/or visual means), thus signifying that the mailed object is safe to be opened. In alternate embodiments of the present invention, the mail verification data further includes additional information (e.g., the contents of the mail object, where it was shipped from, who it was shipped to, etc.).

Such an embodiment could prove extremely useful in receiving mail objects from foreign countries. For example, a secure facility could be located

abroad. Agents of the facility could then be used to inspect the contents of a mail object (e.g., before the mail object is sealed), affix mail ID data to the mail object, and provide the mail ID data to a mail ID device (e.g., a computer, etc.). The mail ID device could then be adapted to store the mail ID data in a database (e.g., a local database, a central database, etc.), and to transmit mail verification data if data subsequently received (e.g., over the Internet) corresponds to the data stored in the database. This embodiment could also prove useful for mail objects (regardless of their origin) directed toward government agencies (e.g., the Federal Bureau of Investigations (FBI), the United States Patent and Trademark Office (USPTO), etc.). Therefore, because at least one embodiment of the present invention could be used to fight terrorism (or to counter terrorism), the Applicant's Petition for Special Application Status should be granted. To the extent additional information is need, the Examiner is encouraged to contact the Applicant at the number listed below.

Respectfully submitted,

Date: September 2, 2003 /s/ Todd Fitzsimmons
Todd Fitzsimmons
Applicant
Registration No. 44,683

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-7522

**DECISION ON PETITION TO MAKE SPECIAL
(COUNTER TERRORISM)
(OCTOBER 8, 2003)**

THE UNITED STATES PATENT
AND TRADEMARK OFFICE

In re application of
Todd E. Fitzsimmons
Application No. 10/271,471
Filed: October 15, 2002
For: SYSTEM AND METHOD FOR MAIL
VERIFICATION

This is in response to the renewed petition filed on September 2, 2003 to make the above-identified application special on the basis of inventions for countering terrorism as set forth in MPEP § 708.02 XI.

The requirements for granting special status under this section are: (A) a petition to make special accompanied by the fee set forth in 37 CFR 1.17(i); and (B) a statement explaining how the invention contributes to countering terrorism.

Applicant's declaration explains that the invention reduces the risk of terrorist attack by providing a system and method of verifying or authenticating a mail object before the mail object is opened and thereby minimizing the recipient's exposure to the contents of the mail object by indicating that the mail object is safe to open or not safe to open via da-

ta comparison by the recipient from a secure facility. This is an acceptable explanation of how the invention would act to counter terrorism.

Since all of the requirements for special status under MPEP § 708.02 XI have been met, the petition is **GRANTED**.

The examiner is directed (1) to make an interference search for possible interfering applications, (2) to promptly examine this application out of turn, and (3) if any interference application is discovered, to examine such application simultaneously and state in the first official letter of such application that it is being taken out of turn because of a possible interference.

Petitioner is advised that this application will continue to be special, through its entire prosecution and pendency, including interference or appeal, if any, only if petitioner makes a prompt and **bona fide** effort, in response to each Office action, to place the application in condition for allowance, even if it is necessary to conduct an interview with the examiner to accomplish this purpose.

SUMMARY: Petition to Make Special **GRANTED**

/s/ Kenneth J. Dorner

Kenneth K. Dorner
Special Programs Examiner
Technology Center 3600
(703 308-0866

**RECORD OF ORAL HEARING
UNITED STATES PATENT AND
TRADEMARK OFFICE
(JUNE 8, 2010)**

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex Parte TODD E. FITZISMMONS

Appeal 2009-013527
Application 10/271,471
Technology Center 3600

Before: HUBER C. LORIN, BIBHU R. MOHANTE,
and CAROLYN D. THOMAS, *Administrative Patent
Judges*

APPEARANCES:

ON BEHALF OF THE APPELLANT:

TODD E. FITZSIMMONS, ESQUIRE
O'Melveny & Myers, LLP
400 South Hope Street
Los Angeles, California 90071-2899

The above-entitled matter came on for hearing Tuesday, June 8, 2010, commencing at 10:41 a.m., at the U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia, before Deborah Courville, a Notary Public.

THE USHER: Calendar No. 5, Appeal No. 2009-013527, Mr. Fitzsimmons.

JUDGE LORIN: Thank you very much.

THE USHER: Are you done with the projector?

JUDGE LORIN: Yes, we are. All right. Good morning, counsel.

MR. FITZSIMMONS: Good morning, Your Honor.

JUDGE LORIN: Could you please state and spell your name for the court reporter, please?

MR. FITZSIMMONS: Sure, Your Honor. My name is Todd Fitzsimmons. That's T-o-d-d, last name Fitzsimmons, F-i-t-z-s-i-m-m-o-n-s.

JUDGE LORIN: All right, counsel. I know you have two appeals before us in a row?

MR. FITZSIMMONS: Correct, Your Honor.

JUDGE LORIN: If you could talk to each of them separately – I mean, there is no problem going to the second one and incorporating your remarks on the first one, but we'll take a pause between the two so that there'll be separate transcripts for each.

MR. FITZSIMMONS: Thank you, Your Honor.

JUDGE LORIN: So if you would start with the first one, which is 2009-013527, you have 20 minutes. When you're ready, you may proceed.

MR. FITZSIMMONS: Your Honor, is this the one ending in Serial No. 471, the first --

JUDGE LORIN: That is correct.

MR. FITZSIMMONS: Okay.

JUDGE LORIN: The one ending in 471. That is correct.

MR. FITZSIMMONS: Thank you, Your Honor. Your Honor, my name is Todd Fitzsimmons. I'm not only the Inventor here, but I'm also a patent attorney with the Law Firm of O'Melveny and Myers. Today, I'll be referring to select pages of the evidence, which I've actually put together in a binder. If it pleases the Court, I do have extra copies for Your Honors.

JUDGE LORIN: I will approve that as long as what's in those binders is already in the record.

MR. FITZSIMMONS: It is, Your Honor, with the exception of some highlights just to accentuate certain language.

JUDGE LORIN: Okay. That's fine.

MR. FITZSIMMONS: Shall I approach the bench, Your Honor?

JUDGE LORIN: Yes, please, Thank you very much.

MR. FITZSIMMONS: Now, Your Honors, the application here before us claims priority to a provisional application that I filed in October in 2001. As you may recall, after the terrorist attacks of 09/11, there were some Anthrax attacks, where Anthrax spores were mailed to media outlets and to U.S.

Government officials. It was in response to those attacks that I filed the provisional application.

The provisional application is directed toward a system and method of verifying a mail object. It does this by using a single set of encoded data, which includes a unique identifier that is then used to identify, or verify, that the mail object came from an identifiable entity. In fact, this can be seen in the system on Figure 1, which is on Page 1 of the handout that I provided you.

As you can see there, System 110 is used to store mail identification data, which can include a unique identifier in a database. It's then affixed to a mail object, at Reference No. 132. The mail object is then provided to a recipient, where the mail identification data is scanned by a Device 120 and communicated to the Device 110 over a Network 102.

The provided mail identification data is then compared to the stored mail identification data, and if there is correspondence, mail verification data can either identify that the mail object came from an identifiable source or it can provide additional information like sender data, and so forth.

Now, in one embodiment of the invention, the application provides that the sender can actually generate, or create the unique identifier. The problem when you have a sender generating, or creating, the unique identifier is that there is no assurance that the identifier is indeed unique. You can image different senders using the same identifier on the same mail object, thus defeating the purpose.

So the solution in the industry is to not allow the sender to generate, or create, the unique identifier.

This is done by the mail carrier. So for example, if you go to FedEx, FedEx will generate a unique identifier or a tracking number. The same is true for UPS Airborne, DHL, and so forth. So the application solves the problem of how do you allow the sender to generate a unique identifier, and they also ensure that that identifier is truly unique enough to track or identify the mail object. And it does this by concatenating data onto the center-generated identifier.

So for example, you can concatenate sender data, which would identify the sender of the mail object, onto the sender-generated identifier, and that would allow you to distinguish the mail object from objects sent by other senders. You could concatenate recipient data, which would allow you to distinguish the mail object from objects sent to different recipients. You could concatenate shipping data to distinguish mail objects that were sent on different dates from different locations, and so forth. In fact, in one embodiment of the invention, the claims concatenate both sender data, recipient data, and shipping data onto the sender-generated identifier to create a truly unique identification number, if you will.

In fact, this is shown in Claim 10 of 471 application, which is on Page 2 of the handout that I provided you, highlighted portions indicating some of the relevant text. And as you can see from Claim 1, the mail identification data, which is affixed to the mail object comprises a single set of encoded data, and that single set of encoded data, a bar code, for example, would include four values, the sender-generated identifier, sender data, recipient data and shipping method data. That information is then stored in a database. It is then scanned at the recipient, com-

municated over the network and compared to the previously stored data in order to determine whether mail verification data should be provided.

And if you look at Claim 10 in conjunction with Claim 1 -- Claim 10 is a dependent claim from Claim 1 -- it provides that the portion that is stored provided over the network and compared is indeed all four portions of those data. I used Claim 10 as an example, because it's not only a narrow embodiment. It's a preferred embodiment. And it's also clearly distinguishable over the cited art.

The claims were rejected by the Examiner over Musgrave, and some of the dependent claims were rejected over Musgrave in view of Li. Now, neither of these references actually discloses a center-generated identifier where data is concatenated onto that identifier to render a unique identifier that can be used to verify the mail object.

What Musgrave does, Musgrave uses iris data. Now, iris data is like a fingerprint. It uniquely identifies an individual. And they use that iris data on the face of the mail object to identify either the sender or the recipient of the mail object. In fact, on Page 3 is the cover page of Musgrave, where the abstract provides a very clear description of what's being done in Musgrave with respect to iris data. I won't read it for you, but what is taking place here, and it's described throughout Musgrave, is that if you want to identify the sender, you put the sender's iris data, a digital representation of the iris data, on the mail object. You can then compare that information to information that was previously stored during an enrollment period to verify who the sender was of the

mail object. You can also put the recipient's iris data on there, and when the package is being delivered, you can scan the recipient's eye and compared that to what's printed on the face of the envelope to identify whether you're indeed providing it to the proper recipient.

So there is no disclosure because they're only using the iris data. There is no disclosure of a sender-generated identifier. I guess one could argue that the iris data itself is sender-generated to some degree even though it's biometric data about the sender. But there is clearly no step of concatenating data onto that to render it unique. There is no need to. The iris data is disclosed in Musgrave as being a truly unique value in and of itself to perform the function of identifying the sender or the recipient.

So Musgrave does not anticipate the claimed language. In fact, the Examiner doesn't argue that. He argues that it would be obvious. However, it's not sufficient to merely state that something is obvious. You must provide reason and rationale as for that obviousness. In fact, the court in KSR v. Teleflex (ph.) stated that rejections on obviousness grounds cannot be sustained by mere conclusory statements. Instead, there must be some articulated reasoning and some rational underpinning to support the legal conclusion of obviousness.

And, here, the Examiner provided no reasoning or rationale whatsoever. With respect to the 471 application, what he does is he acknowledges the deficiencies of Musgrave and says, yeah, Musgrave does not disclose the mail identification data that includes these four values or the fact that those four

values are being used to verify the mail object. But he says that that -- those limitations are entitled to little or no patentable weight. And he states that because he identifies them as “descriptive material.”

And for this proposition, he cites to *In re Lowry*. *In re Lowry* deals with printed matter cases. The court describes printed matter as being printed lines or characters useful and intelligible only to the human mind. But then *In re Lowry* further goes on and says that the printed matter cases have no factual relevance where the invention, as defined by the claims, requires that the information be processed not by the mind, but by the machine, a computer.

That’s exactly the case here. The mail identification data is not merely printed or affixed onto the mail object. It is then scanned, communicated over a network, compared to information stored in a database to retrieve mail verification data. This is processing and thus, this is not printed matter, as identified by the Examiner.

Now, to the extent -- I’m not sure that the law supports this, but to the extent one could say, “Well, it’s just kind of inherently obvious over *Musgrave* because *Musgrave* is kind of similar art,” I would strongly disagree with this. In fact, first of all, there is no motivation at all to concatenate any data onto the iris data identified in *Musgrave*, because the iris data in and of itself is sufficient to perform the function of identifying the sender or the recipient.

And you would not add data to the face of the mail object just for no reason at all. This is especially true in light of the fact that you have to keep in mind, a mail object has a limited amount of real es-

tate. The whole objective is to put as little information on the mail object as possible to leave the real estate open for advertising and other functionalities in order to perform the desired function. Same is true for how much data you want to store in a database for tracking a mail object, and so forth. It's to minimize the data, not to maximize the data. So there is no motivation to go in that direction unless there is some additional functionality which has not been identified.

Now, one thing to point out is that Musgrave uses iris data to identify the sender or the recipient of the mail object. They do not use it to track a mail object or to identify the mail object, which it really can't be done to a very good degree, because, as you can imagine, two mail objects sent from the same sender would have the sender's iris data and you could not distinguish one over the other.

So the question is maybe in Musgrave, how do they identify a mail object for tracking purposes. And Musgrave states, and this is in Musgrave on Page 14, Line 30, through Page 15, Line 2, that if you want to track the mail object, the mail object should include "a tracking number or other unique shipping number generated by the carrier." That's the prior art we were talking about earlier. Thus, not only does Musgrave not disclose the whole step of concatenating and using that to then verify the mail object, but there is no motivation, and it clearly teaches away by teaching that you would use the prior art carrier-generated tracking number in order to track or identify a mail object.

Now, the Examiner spends a great deal of time pointing out where the four different values, sender data, recipient data, and so forth, can be found in Musgrave. First of all, the invention is not the existence of those four data values on a mail object. All mail objects have some sender data, have some recipient data. I shouldn't say all, but most, I guess. Obviously, there is a recipient's name and address, things of that nature. But the claimed invention is not the existence of that four data values, but it's the existence of those four data values in a single set of encoded data, which can be easily retrievable, and the use of that data to then verify that the mail object was sent by an identifiable entity.

In fact, again, going back to the KSR case, they state that a patent composed of several elements is not proved obvious merely by demonstrating that each of the elements was independently known in the prior art. That is the case here. While Musgrave may disclose various data values on a mail object, they do not -- it does not disclose them in a single set of encoded data or use them to verify the mail object.

Now, the Li reference is cited for some dependent claims, but it's actually an interesting reference in that Li actually addresses the issue that is being addressed here in this application. What do you do when you have a sender-generated identifier which is not necessarily unique. In fact, Li addresses this concern in the background of the invention section and says that "carriers may consider this to be unacceptable since they would have to rely on the quality of the sender-generated number for tracking mail items through their system."

So Li acknowledges the same problem in the art. How does Li solve that problem? Li says here is what you do. Let the sender generate an identifier. Doesn't even have to be unique. They can then submit the identifier. You will link that in a database to the carrier-generated identifier, the prior art. The carrier-generated identifier is then attached to the mail object and actually used to track the mail object to the system. And the sender-generated identifier is only used for communications or correspondence back with the sender. It is not used to track the mail object, and therefore, Li clearly teaches away from the claimed invention by going in another different direction with respect to that problem.

So in sum, we have neither reference disclosing the claimed invention, both references teaching away from the claimed invention. I would argue that any argument of obviousness over these references is not only impermissible hindsight, based on the claims at issue in this application, but it's contrary to the law of teaching away, which I won't bore the Court with citations to the case law on that, but, you know, the courts have found that references that teach away from the claimed invention do not render the claimed invention obvious.

Now, I will briefly discuss some of the claims that are at issue in the 471 application. Claim 1, again, is reproduced on Page 4 of the handout. And, again, you'll see the relevant claims in the rest of this handout with highlighted portions. Claim 1, as we went over a minute ago, has the mail identification data where there is a single set of encoded data, which includes the four values, and then a portion of

that data is stored in a database. It is later retrieved, provided over a network and compared.

The difference between Claim 1 in its dependent claims primarily is that the portion that is stored, provided and compared in Claim 1 is described as being at least the sender data. So at least that piece of concatenated data. If we turn the page to Page 5, you'll see Dependent Claims 7 through 10, which provide that different portions are provided -- different portions are stored, provided and compared. So Claim 7, for example, in addition to the sender data, there is also the sender-generated identifier that is stored, provided and compared. Claim 8, it's sender data and recipient data. Claim 9 it's sender data and shipping method data. And Claim 10, as previously discussed, is all four data values.

Now, while Claim 10 is clearly distinguishable in that its got these four values that are then used to distinguished and render a unique value that could be used to distinguish or identify a mail object, the other dependent claims in Claim 1 are also distinguishable. And I say this because the prior art, it teaches a single unique value. It does not teach a situation where a sender provides a non-unique value and you have to concatenate data onto that in order to render a unique value. It doesn't matter whether the concatenated data is one data value, two, three, four, and so forth. It's the whole concept of using the concatenated data to track or verify a mail object is not disclosed in the art. And for that reason, Claims 7, 8, 9, those are distinguishable over the art as well.

There is really no need to go into the other independent claims, which is 22 and 36, because they are similar to Claim 1 with respect to the relevant limitations. And the same is true for most of the dependent claims. Page 7 and 8 is dependent claims and Claim 22. And, again, on -- like on Page 8, for example, Claim 75 uses three pieces of the data to verify the mail object. Claim 76 uses four pieces of data. And just different portions are recited in those claims. On Page 10 is dependent claims to 36, which is Claims 42 through 44, and, again, 43 uses three pieces of data, 44 uses four pieces of data, and so on. On Pages 11 and 12 and 13 are other dependent claims, which I won't go into because I believe these dependent claims are sufficiently briefed as to their distinctions over the prior art.

And, Your Honor, with respect -- I would close with respect to the 471 application by pointing out something that's kind of unique with respect to the file history, or the prosecution history in this case. This case was originally assigned to a Primary Examiner Cosimano. The Primary Examiner, after an Office Action, identified that many of these claims were allowable over the art. And for some reasons, the application was then reassigned. I don't know if Mr. Cosimano retired or what the situation was, but it was reassigned to a first-year Examiner, John Bass, who issued rejections over a first set of art. I took issue with those rejections, filed an Appeal Brief and a Notice of Appeal. Mr. Bass -- then withdrew the rejections, reopened prosecution. Mr. Bass, was, my understanding, was terminated. I don't know the reasoning behind that --

JUDGE LORIN: Okay. Counsel, I don't want to get into this whole discussion of what happened in the patent examining --

MR. FITZSIMMONS: Okay.

JUDGE LORIN: Okay. We're just dealing here with the legal issues that you've raised in the Brief, okay? That's something -- if you have a concern with the Patent Office, that's something you bring up with them, okay? This isn't --

MR. FITZSIMMONS: Okay, No. I --

JUDGE LORIN: This isn't the tribunal to do that.

MR. FITZSIMMONS: I understand.

JUDGE LORIN: Let me ask a question about this claim here, because I did see that the Examiner raised the issue of nonfunctional descriptive material.

MR. FITZSIMMONS: Yes.

JUDGE LORIN: If I understood what you're saying, is that the distinctive aspect of your invention is this string, single set of encoded data, and that it includes a unique identifier, sender data, recipient data, and shipping method data?

MR. FITZSIMMONS: Correct. Where the unique identifier is generated by the sender, correct. That's the ending of the first paragraph of affixing.

JUDGE LORIN: Well, it says the unique identifier consists of a numeric value assigned by the sender?

MR. FITZSIMMONS: Correct.

JUDGE LORIN: Okay.

MR. FITZSIMMONS: And there is different language in different claims, but, yes, assigned by the sender in this case.

JUDGE LORIN: Right. Well, it's important what these words mean, and that's my question to you. Are there definitions in the specification for each of these terms? For instance, what's the difference between sender data and recipient data?

MR. FITZSIMMONS: Well, the sender data is actually defined in the claim language, I believe, and if it's not in this claim, it's in other claims. But the sender data was defined in the claim language, in other independent claims, as being data that can be used to identify the sender. And recipient data is information that can be used to identify the recipient. Those values are very broad values. And shipping method data, obviously, is pertaining to the method of shipment for the mail object. And the unique identifier is assigned by the sender, or in the specification, it talks about being generated by the sender.

JUDGE LORIN: Well, so you're agreeing with the Examiner that each one of these sets of data that you're stringing together is simply information?

MR. FITZSIMMONS: Well, it's not printed matter, and the reason is, is because if you were to stop after the first limitations, the affixing of the mail data on the object, I would agree, because then there is nothing being done with that information other than just affixing it on the mail object. But what's happening is a portion, that single set of encoded data is referred to as mail identification data. And later on in that claim, a portion of the mail identification data is stored, and another portion of that mail identi-

fication data is received and provided over the network. And there is a comparison done with respect to the portion.

Now, the Examiner's position, we had many interviews with respect to this subject. And the Examiner's position was, well, it's a portion of the data. It doesn't identify which portion. Now, I would say that the case law doesn't require -- as long as there is -- this information is being used, it doesn't necessarily require that you identify, you know, one portion versus another. This information is not being used or processed by the human mind. It's being processed by a computer. But even if the Examiner wanted to take the position that, well, it is printed matter because only the sender data is referred to in Claim 1 as being stored, provided and compared, that doesn't answer the issue with respect to Claim 10.

Claim 10 -- and I'm taking an extreme position -- but Claim 10 is one of the more narrow claims, where all four data values are stored. All four data values are not only affixed, but are then processed by the computer through their comparison steps, they're absolutely not printed matter. And that's clear by *In re Lowry*, which distinguishes something that's processable by a human mind versus processable by a computer. These are computers that are doing this, correspondences and communication of this information.

So what I was discussing during the interviews with the Examiner was Claim 10 is clearly not printed matter. So let's start there and kind of work our way backwards, and we can address those issues perhaps as they get back towards Independent

Claim 1. Again, with respect to the sender data, which is actually being described as being, you know, communicated over the network, I would agree that - or I would say that that is clearly not printed matter because it's being processed.

But, again, the point of novelty here is not so much -- I mean it is a distinguishing feature -- I'll give you that -- that there is this single one of encoded data, but it's how you use that encoded data. And so, again, if you look at Claim 10, that -- those four data values are being stored, communicated over a network and then compared. And if you look to, say, Claim 9 or 8 or 7, there are different data values. It might be sender data and the unique identifier that's assigned by the sender. Those are the values that are stored, communicated, and compared.

So, again, even to the extent one -- the Examiner wants to argue that just the affixing of the data somehow printed matter, which I disagree with that position, you can't say it's printed matter when it's being processed, which is what's taking place, at least, to portions of it in the dependent claims and even in the independent claims.

JUDGE LORIN: Right. Let me stop you there for a second.

MR. FITZSIMMONS: Okay.

JUDGE LORIN: Okay. I can see the Examiner's position with regard to affixing. And then I can see your position after that. But after the affixing step of the method, you then say "receiving at least an authenticating portion"?

MR. FITZSIMMONS: Correct.

JUDGE LORIN: What does that mean?

MR. FITZSIMMONS: Well, that was -- at the time, it was meant to distinguish -- I mean, I could have said a first portion, but I said "an authenticating portion" because that's the way it was described in the specification. It's a portion. It's a portion. What you're doing is, in essence, you've got this single set of encoded data that includes these four values. Preferably, you would take all four values. That would be the first portion. And you would be storing it in a database. You would then be retrieving those four values, communicating over a network and then comparing them. But because the stored values are basically the same as the retrieved values, and I was going to -- I didn't want to confuse the reader with respect to whether they were indeed the same values, and so forth -- because they don't have to be. Obviously, if there is no correspondence, then mail verification would not be presented. So, again, the authenticating portion and the other portion, which is the --

JUDGE LORIN: Verification?

MR. FITZSIMMONS: -- verification portion is just a first portion and a second portion. There is nothing magic. Again, it's just the way the specification describes the portions, so --

JUDGE LORIN: Well, that's important because the single set includes at least. So you could have other information in that set?

MR. FITZSIMMONS: Correct.

JUDGE LORIN: And that means the authentication portion and the verification do not need to be one of the four in your string?

MR. FITZSIMMONS: I understand that that could be the case, and that's why it is specifically called out in Claim 1 that the portion does include at least the sender data. And that's why in Claim -- I believe it's 6 -- it's called out as not only being sender data, but it's also -- I'm sorry. It's Claim 7. It's called out not only being sender data, but also being the sender-generated, or sender-assigned, unique identifier. And in Claim 8, it's called out as not only being sender-data, but recipient data, and in Claim 9 -- you know, and so forth, until you get to Claim 10, where you --

JUDGE LORIN: I see.

MR. FITZSIMMONS: So it does call out and specifically -- and some of those limitations were actually added after an interview with the Examiner on this exact same point, because the Examiner had a concern. My concerns were that someone might tweak a little bit and with what was being stored and what was being provided in order to not infringe the claims. The Examiner's position was, well, if you don't define some portion as actually being stored or communicated, then I might have some issue with respect to the printed matter case. So that's why all these limitations were added in there.

And I thought we had an agreement as with respect to distinguishability over the prior art. But the printed matter argument just kept getting repeated, as it was kind of cut and paste situation, and I got nowhere with respect to that when I discussed it

with the Examiner even though we now have distinct portions that are being processed, which is contrary to the printed matter case, as discussed in In re: Lowry.

JUDGE LORIN: Well, if I understand your position, yes, yes. With regard to Lowry, I understand your position really centers around the authentication portion, that there is a portion of the information that has a function and that is to authenticate, and another function is to verify.

MR. FITZSIMMONS: Yes.

JUDGE LORIN: And that's being done by via the network. That I think is what your position is?

MR. FITZSIMMONS: Correct. And the fact that the claim language calls out what those portions are at least including --

JUDGE LORIN: In the dependent claims --

MR. FITZSIMMONS: Yes. Well, and even in the independent claim, it's called out as including at least sender data, which as I said kind of during the argument, the sender data is a concatenated piece of data onto the unique identifier. Now, I would agree that, really, the value in this starts to come when you start to put at least two pieces of data together, like the sender data with the sender-assigned unique identifier, which is Claim 7. And so you start to compile at least more than one.

And that's why when I was presenting this to the Examiner, I gave him this kind of spectrum, if you will. And we went from extremely narrow with Claim 10 to rather broad with Claim 1. And I figured that we would identify where he found the distinc-

tion to be. And I figured it would probably be at least Claim 7, but perhaps it was an argument to Claim 1 because it did have the single set of encoded data with the four values, and so forth. But the Examiner, you know, if you look again at his rejection of Claim 1, he doesn't really identify, or doesn't discuss how these values are used in Musgrave. He just says, oh, there's some recipient data. There is some sender data. And with respect to Claim 7, 8, 9 and 10, he just kind of off the cuff just says, oh, they're obvious. How? You know? And doesn't acknowledge the fact that now it's not printed matter, and so forth. So it leaves a lot to wonder.

JUDGE LORIN: Al right. Understood, counsel. Thank you. Thank you for your input.

Any further questions? No?

Thank you. We'll take a short break.

Whereupon, the proceedings, at 11:11 a.m., were concluded.

110a



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**

FOREIGN PATENT DOCUMENTS

JP 09-99931 * 4/1997

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

(Continued)

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

OTHER PUBLICATIONS

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

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

(Continued)

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

Primary Examiner—Fadéy S Jabr

(65) **Prior Publication Data**

(57) **ABSTRACT**

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**

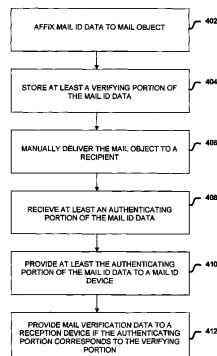
U.S. PATENT DOCUMENTS

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)

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



111a

US 7,818,268 B2

Page 2

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 Security", Security Management,
Nov. 1998, pp. 1-10.*

* cited by examiner

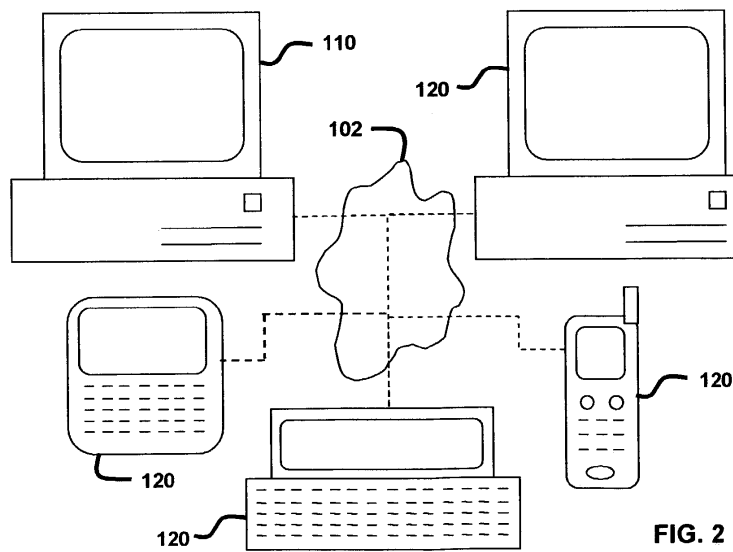
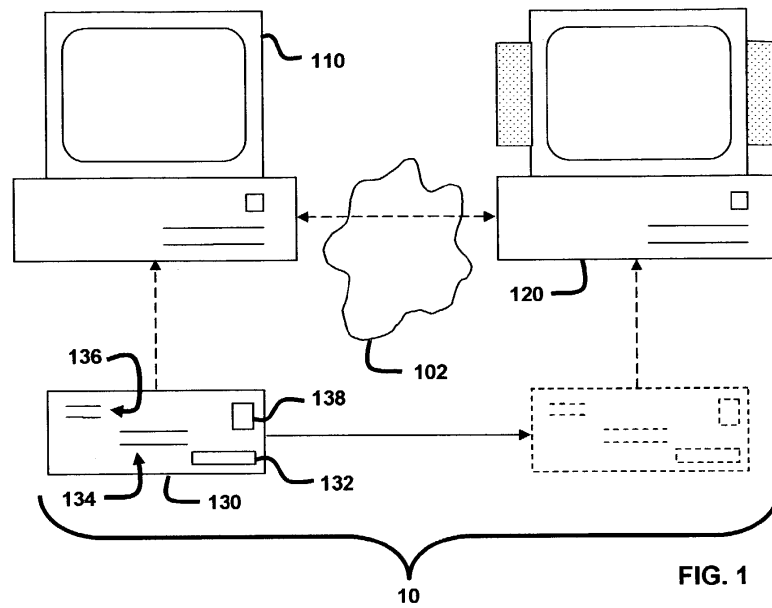
112a

U.S. Patent

Oct. 19, 2010

Sheet 1 of 3

US 7,818,268 B2



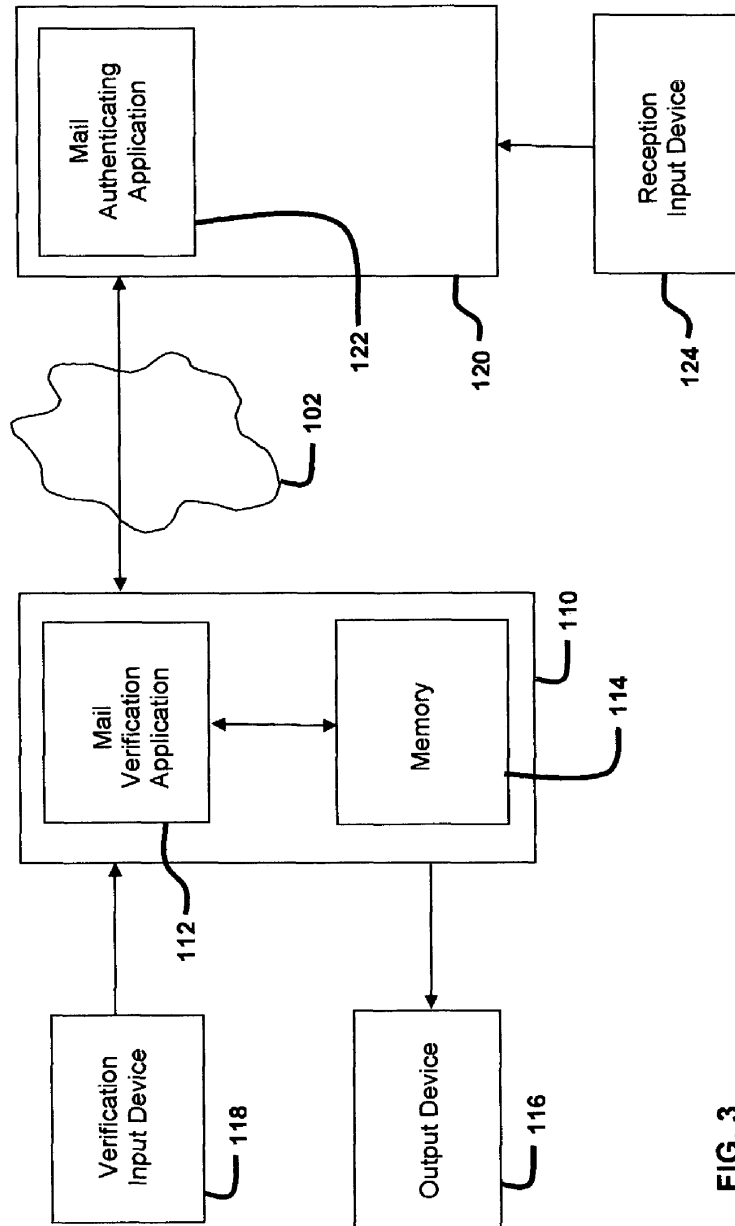


FIG. 3

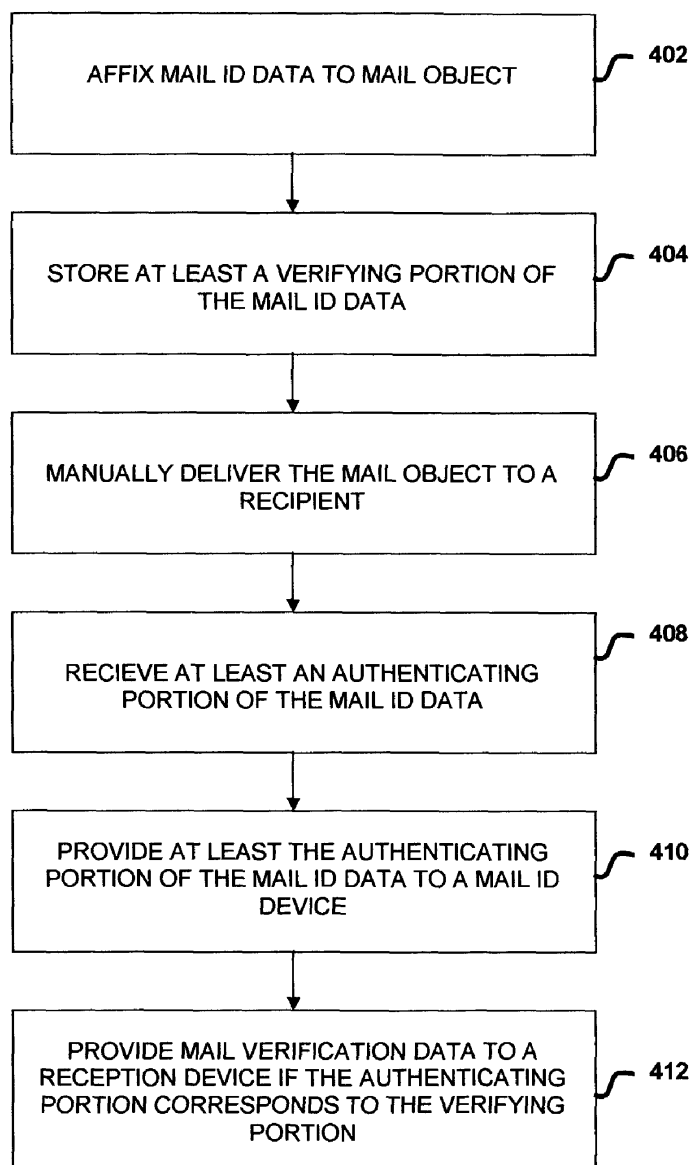


FIG. 4

US 7,818,268 B2

1

**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

2

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.

3

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 appreciated, as depicted in FIG. 2, that the reception device(s) 120 includes, but is not limited to, personal computers, set top boxes, personal digital assistants (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,

4

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 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 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 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.

5

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 pro-

6

vides 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.

7

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.

8

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:

9

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 infor-
 mation, recipient information and shipping method
 information, wherein said unique identifier con-
 sists 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 authenticat-
 ing portion comprises at least said sender informa-
 tion and said shipping method information; and
 provide mail verification data via said network if at
 least said authenticating portion of said mail iden-
 tification 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 com-
 prising an output device adapted to affix said mail identifica-
 tion 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 iden-
 tification 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 iden-
 tification data on at least one tag.

38. The mail verification system of claim 33 further com-
 prising an input device adapted to receive at least said ver-
 ifying 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.

10

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 informa-
 tion.

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 iden-
 tification data.

50. The mail verification system of claim 33, further com-
 prising 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 authen-
 ticating 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 dis-
 play 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.

* * * * *



US009105002B2

(12) **United States Patent**
Fitzsimmons

(10) **Patent No.:** **US 9,105,002 B2**
(45) **Date of Patent:** ***Aug. 11, 2015**

(54) **SYSTEM AND METHOD FOR PROVIDING INFORMATION TO A RECIPIENT OF A PHYSICAL MAIL OBJECT**

G06Q 30/02 (2012.01)
H04L 12/58 (2006.01)
H04W 4/12 (2009.01)

(71) Applicant: **Todd Fitzsimmons**, Gardena, CA (US)

(52) **U.S. CL.**
CPC *G06Q 10/083* (2013.01); *G06Q 10/0832* (2013.01); *G06Q 10/107* (2013.01); *G06Q 20/382* (2013.01); *G06Q 30/0241* (2013.01); *H04L 12/585* (2013.01); *H04L 5/12* (2013.01); *H04W 4/12* (2013.01)

(72) Inventor: **Todd Fitzsimmons**, Gardena, CA (US)

(73) Assignee: **Secured Mail Solutions, LLC**, Las Vegas, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(58) **Field of Classification Search**
CPC . *G06Q 10/083*; *G06Q 10/107*; *G06Q 20/382*; *G06Q 30/0241*; *G06Q 10/0832*; *G06Q 10/08*; *G06Q 10/10*; *G06F 17/00*
USPC 235/375, 487, 462.01; 705/401–402, 705/408, 1.1, 64
See application file for complete search history.

(21) Appl. No.: **14/528,675**

(56) **References Cited**

(22) Filed: **Oct. 30, 2014**

U.S. PATENT DOCUMENTS

(65) **Prior Publication Data**

US 2015/0066796 A1 Mar. 5, 2015

2003/0110144 A1 * 6/2003 Sansone 705/406
2004/0143650 A1 * 7/2004 Wollowitz 709/219
2008/0291486 A1 * 11/2008 Isles et al. 358/1.15
2009/0119219 A1 * 5/2009 Bleumer 705/62

* cited by examiner

Related U.S. Application Data

(63) Continuation of application No. 13/848,370, filed on Mar. 21, 2013, now Pat. No. 8,910,860, which is a continuation of application No. 13/560,306, filed on Jul. 27, 2012, now Pat. No. 8,429,093, which is a continuation of application No. 13/297,515, filed on Nov. 16, 2011, now Pat. No. 8,260,629, which is a continuation of application No. 12/454,052, filed on May 11, 2009, now Pat. No. 8,073,787, which is a 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.

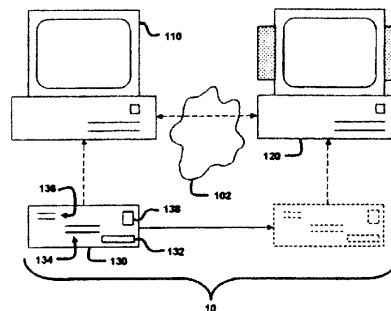
(51) **Int. Cl.**
G06F 17/00 (2006.01)
G06Q 10/08 (2012.01)
G06Q 10/10 (2012.01)
G06Q 20/38 (2012.01)

Primary Examiner — Edwyn Labaze

(57) **ABSTRACT**

A system and method is provided for transmitting information over a wide area network, such as the Internet, in response to receiving at least a portion of mail data. In one embodiment of the present invention, information is stored in a memory. Mail data is then affixed to a mail object. The mail object is then manually delivered to a recipient. The mail data is then provided to a reception device. The reception device then uses the mail data to retrieve the information from a mail device in communication with the memory. In a preferred embodiment, the mail data includes data corresponding to the recipient of the mail object, and the information includes data that identifies the recipient of the mail object and data that corresponds to a content of the mail object.

20 Claims, 3 Drawing Sheets



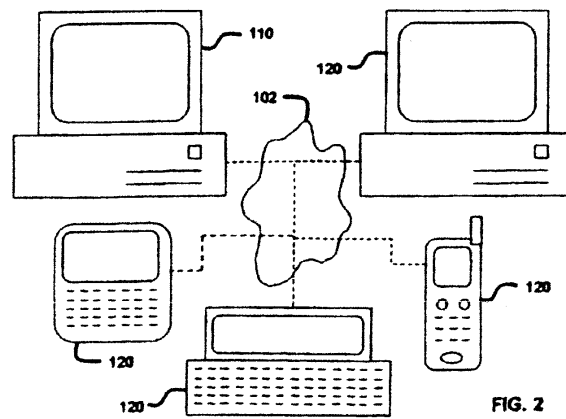
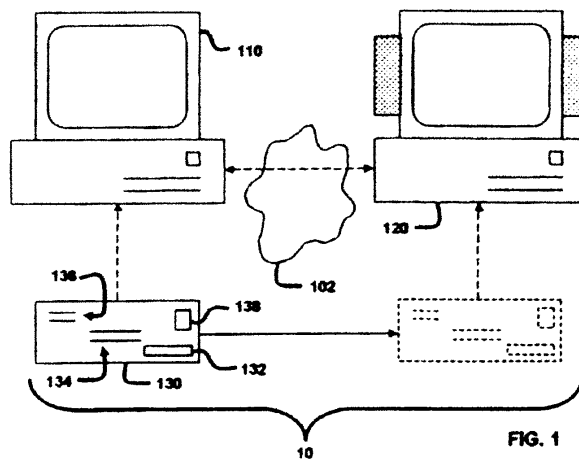
121a

U.S. Patent

Aug. 11, 2015

Sheet 1 of 3

US 9,105,002 B2



122a

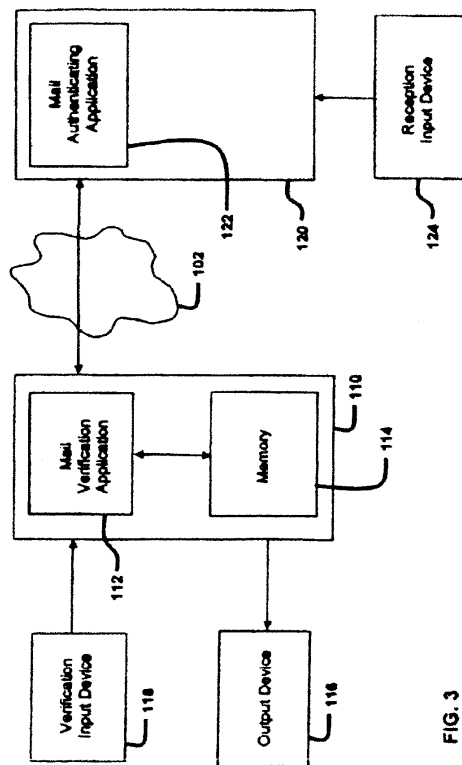


FIG. 3

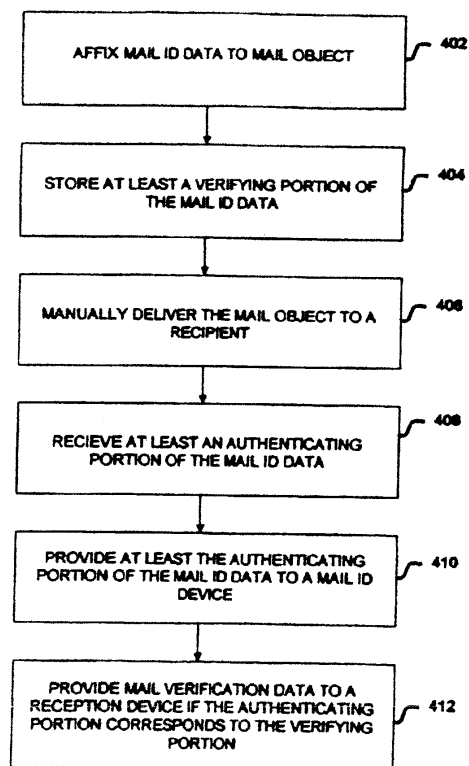


FIG. 4

1
SYSTEM AND METHOD FOR PROVIDING
INFORMATION TO A RECIPIENT OF A
PHYSICAL MAIL OBJECT

CROSS-REFERENCE TO RELATED
 APPLICATION

This application is a continuation of U.S. patent application Ser. No. 13/848,370, filed Mar. 21, 2013, which is a continuation of U.S. patent application Ser. No. 13/560,306, filed Jul. 27, 2012, and issued on Apr. 23, 2013 as U.S. Pat. No. 8,429,093, which is a continuation of U.S. patent application Ser. No. 13/297,515, filed Nov. 16, 2011, and issued on Sep. 4, 2012 as U.S. Pat. No. 8,260,629, which is a continuation of U.S. patent application Ser. No. 12/454,052, filed May 11, 2009, and issued on Dec. 6, 2011 as U.S. Pat. No. 8,073,787, which is a continuation of U.S. patent application Ser. No. 10/271,471, filed Oct. 15, 2002, and issued on Oct. 19, 2010 as 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 provide 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., envelopes, 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

2

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

3

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 appreciated, as depicted in FIG. 2, that the reception device(s) 120 includes, but is not limited to, personal computers, set top boxes, personal digital assistants (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

4

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 include, but is not limited to, the packaging that surrounds the mail object). 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 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 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

5

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 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.

6

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 providing electronic data to a recipient of a mail object, comprising:

using an output device to affix a single set of mail ID data to said mail object, said single set of mail ID data including at least recipient data, said recipient data comprising a personalized network address associated with said recipient of said mail object;
submitting said mail object to a mail carrier for delivery to said recipient of said mail object;
receiving said recipient data from a reception device of said recipient via a network; and
providing by at least one processor said electronic data to said reception device via said network in response to receiving said recipient data, said electronic data comprising a sender's web page that identifies said recipient of said mail object and includes data corresponding to a content of said mail object;
wherein said electronic data is configured to be displayed to said recipient via a web browser on a display of said reception device.

2. The method of claim 1, further comprising providing by said at least one processor a second set of electronic data to a sender of said mail object indicating that said recipient requested said electronic data.

3. The method of claim 2, wherein said second set of electronic data includes at least a portion of said recipient data.

4. The method of claim 2, wherein said second set of electronic data includes data corresponding to said mail object.

5. The method of claim 2, wherein said second set of electronic data includes data corresponding to said mail object.

7

6. The method of claim 1, wherein said step of affixing said single set of mail ID data to said mail object, further comprises encoding said single set of mail ID data prior to being affixed to said mail object.

7. The method of claim 1, wherein said reception device is a cellular telephone.

8. The method of claim 7, wherein said electronic data is formatted for being displayed via a web browser on said cellular telephone.

9. A system for providing electronic data to a recipient of a mail object, said mail object including a single set of mail ID data that includes at least recipient data, comprising:

at least one database for storing at least a first set of electronic data;

a mail device; and

at least one application operating on at least said mail device, said at least one application being in communication with said at least one database and a reception device of said recipient having at least an input device and a display, and being configured to:

receive said recipient data from said reception device, said recipient data including personalized data that can be used to identify said recipient of said physical mail object; and

provide said first set of electronic data to said reception device via said network in response to receiving said recipient data, said first set of electronic data comprising a sender's web page that identifies said recipient and includes data corresponding to a content of said mail object;

wherein one of receiving said recipient data from said reception device and providing said first set of electronic data to said reception device results in a second set of electronic data being provided to said sender of said mail object.

10. The system of claim 9, wherein said at least one application is further configured to encode said single set of mail ID data and to affix said single set of encoded data on said mail object.

11. The system of claim 9, wherein said at least one application is further configured to generate an email addressed to said recipient in response to receiving said recipient data.

12. The system of claim 9, wherein said second set of electronic data includes at least a portion of said recipient data.

13. The system of claim 9, wherein said second set of electronic data includes data corresponding to said recipient of said mail object.

8

14. The system of claim 13, wherein said at least one application is further configured to provide said second set of electronic data to said sender via a web page.

15. The system of claim 9, wherein said second set of electronic data includes data corresponding to said reception device.

16. A system for providing electronic data to a recipient of a mail object, said mail object including a single set of mail ID data that includes at least recipient data, wherein said recipient data corresponds to said recipient of said mail object, comprising:

a processor;

at least one database for storing at least said electronic data; and

at least one application operating on at least said processor, configured to:

affix the single set of mail ID data to said mail object, said mail object being submitted to a mail carrier for delivery to said recipient of said mail object;

at least one other application in communication with at least a reception device of said recipient having at least one input device for receiving said recipient data from said mail object, said at least one other application being configured to:

receive said recipient data from said reception device; and

provide said electronic data to said reception device via a network in response to receiving said recipient data, said electronic data including a sender's web page that identifies said recipient and includes data that corresponds to a content of said mail object;

wherein one of receiving said recipient data and providing said electronic data results in other electronic data being provided to a sender of said mail object.

17. The system of claim 16, wherein said reception device is a cellular telephone.

18. The system of claim 17, wherein said electronic data is formatted for being displayed via a web browser operating on said cellular telephone.

19. The system of claim 16, wherein said other electronic data includes at least one of at least a portion of said recipient data and data corresponding to said recipient of said mail object.

20. The system of claim 16, wherein said single set of mail ID data is encoded before it is affixed to said mail object.

* * * * *