

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

RALLY AG LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 23-1106 (JHS)
	)	
APPLE, INC.,	)	DEMAND FOR JURY TRIAL
	)	
Defendant.	)	

**SECOND AMENDED COMPLAINT FOR
PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL**

Plaintiff Rally AG LLC (“Rally” or “Plaintiff”), for its Second Amended Complaint against Defendant Apple, Inc. (“Apple” or “Defendant”), alleges as follows:

NATURE AND BASIS OF THE ACTION

1. This is an action for patent infringement arising under the laws of the United States, 35 U.S.C. §§ 1 *et seq.* and results from Apple’s unauthorized use of Plaintiff’s patented innovations. Plaintiff seeks monetary damages, injunctive relief, and recovery of its reasonable attorneys’ fees incurred in connection with this action.

2. Plaintiff is the owner of U.S. Patent No. 11,361,107, titled “Privacy Friendly Communications by Operation of Cloaked/Decloaked Email” (“the ’107 Patent” or “the Asserted Patent”). As detailed herein, Apple infringes the Asserted Patent.

PARTIES

3. Plaintiff is a Washington corporation with its principal place of business located at 2205 Carillon Point, Kirkland, Washington, 98003.

4. On information and belief, Defendant Apple is a Delaware corporation with its principal place of business located at One Apple Park Way, Cupertino, California 95104.

5. On information and believe, Defendant has a regular and established place of business at 125 Christiana Mall, Newark, DE 19702. Defendant may be served with process through its registered agent for service of process in Delaware, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

6. Defendant directly and/or indirectly makes, imports, distributes, markets, sells and/or offers to sell throughout the United States, including in this judicial district, products and/or services (the “Accused Products”) that infringe one or more of the claims of the ’107 Patent as described below.

JURISDICTION AND VENUE

7. This is a civil action for patent infringement arising under the Patent Laws of the United States as set forth in 35 U.S.C. §§ 1, *et seq.*

8. This Court has federal subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

9. This Court has personal jurisdiction over Defendant, as a Delaware corporation.

10. Defendant is registered with the Delaware Secretary of State to conduct business within Delaware, and has a regular and established place of business at 125 Christiana Mall, Newark, DE 19702.

11. Defendant directly and/or indirectly makes, imports, distributes, markets, sells and/or offers to sell throughout the United States, including in this judicial district, products and/or services (“the Accused Products”) that infringe one or more claims of the ’107 Patent as described below. The Accused Products include all Apple devices, including iPhones and iPads, that have cloaking and decloaking capabilities as described below.

12. Defendant operates the website <https://www.Apple.com/> and provides a mobile application in order to provide privacy measures to its customers and users, including but not limited to its “Hide-My-Email” feature.

13. Defendant has operated services offered to users in the State of Delaware.

14. Defendant has transacted and solicited business and actively advertised to residents within the State of Delaware.

15. This Court also has personal jurisdiction over Defendant because, in addition to Defendant’s own online website and advertising within this judicial district, Defendant also has made its products and services available specifically within the District of Delaware and actively targets and advertises to residents of the District of Delaware.

16. Accordingly, specific and general personal jurisdiction exists over Defendant. This Court’s personal jurisdiction over Defendant comports with the constitutional standards of fair play and substantial justice and arises directly from the Defendant’s purposeful minimum contacts with the State of Delaware and its infringement of the ’107 Patent.

17. Venue is proper in this Court under 28 U.S.C. §§ 1391(b)-(c) and 28 U.S.C. § 1400(b) because Defendant has committed or induced acts of infringement in this District. In addition, Defendant maintains a regular and established place of business in this District.

18. In addition to the foregoing, venue is proper at least because Defendant, in conjunction with its employees, has committed acts of direct and/or indirect infringement of the ’107 Patent in the District of Delaware at least by practicing the claimed inventions in this Judicial District or contributing to or inducing others to practice the claimed inventions in this Judicial District.

19. Defendant also has committed acts of direct infringement in this District through other Apple employees who have practiced and continue to practice steps of using the claimed system and computer readable medium in this District for development, testing, and/or demonstration purposes.

20. On information and belief, discovery will confirm that Defendant has further directly performed one or more acts using the accused system and computer readable medium in this District.

21. Defendant's products and services, and electronic connections and communications ("the Apple Platform") are accused of infringing the '107 Patent. For example, the technologies underlying the Apple Platform implement the integrated processes by which Apple cloaks and decloaks email communications with customers. On information and belief, discovery will confirm that Defendant has further directly performed one or more steps of using the accused computer readable medium in this District.

DEFENDANT'S INFRINGING METHODS, SYSTEMS, AND PRODUCTS

22. Through the Apple Platform, Defendant makes, uses, sells, offers for sale, coordinates, and/or controls, among other things, its "Hide-My-Email" feature.

23. For example, on information and belief, Defendant makes, uses, sells and offers for sale to its users and customers the Apple Platform, including but not limited to the "Hide-My-Email" feature ("the Accused Products").

24. On information and belief, the Accused Products, including the "Hide-My-Email" feature were introduced with Defendant's iOS 15 platform in or around September 2021. According to Defendant, the "Hide-My-Email" product "lets you create unique, random email

addresses that forward to your personal inbox so you can send and receive email without having to share your real email address.”

25. Further, on information and belief, according to Defendant’s own website, with the Accused Products, “[i]f you create an account with an app or visit a website that supports Sign in with Apple, you can choose to share your email address, if you’re familiar with the app or visit a website, or hide your email address, if you’d prefer more privacy.”

26. Further, on information and belief, according to Defendant’s own website, “[i]f you choose the Hide My Email option, only the app or website you created the account with can use this random email address to communicate with you.”

27. Further, on information and belief, Defendant’s own website provides that, “[w]ith an iCloud+ subscription, you can generate unique, random addresses on your device with iOS 15, iPadOS 15, or macOS Monterey or later in any email field in Safari. You can also generate email addresses on-demand in the Settings app in iOS or iPadOS, in System Settings or System Preferences in macOS, in the Mail app, or on iCloud.com. in iOS 16 or iPadOS 16 or later, you can also keep your email address private in third-party apps.”

HISTORY OF EMAIL AND PRIVACY TECHNOLOGIES AND THE STATE OF THE ART AS OF THE EFFECTIVE FILING DATE OF THE ’107 PATENT

28. Simple Mail Transfer Protocol (SMTP) is an Internet standard communications protocol for email transmission that is widely used across the world.¹ “Email

¹ Sheikh, S. A., Banday, M. T., *Multi-Recipient E-mail Messages: Privacy Issues and Possible Solutions*, 21 AECE 115, 117 (Nov. 30, 2021), available at <https://aece.ro/abstractplus.php?year=2021&number=4&article=13> (last accessed Jan. 1, 2024) (hereinafter, “Sheikh”).

clients, servers and relays use this protocol to communicate with each other making up the email infrastructure.”²

29. SMTP protocols provide a general format for email messages. For example, an email message from one person to another “has a single author, John Doe, a single recipient, Mary Smith, a subject, the date, a message identifier, and a textual message in the body.”³

```

-----
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
So, "Hello".
-----

If John's secretary Michael actually sent the message, even though
John was the author and replies to this message should go back to
him, the sender field would be used:

-----
From: John Doe <jdoe@machine.example>
Sender: Michael Jones <mjones@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
So, "Hello".
-----

```

30. Similarly, SMTP protocols provide a general format for email reply messages. For example, in a conversation thread between John and Mary, “John first sends a message to Mary, Mary then replies to John’s message, and then John replies to Mary’s reply message.”⁴

² *Id.*

³ Resnick, P., “Internet Message Format”, RFC 5322 – Appendix A-1, Network Working Group, Qualcomm Incorp. (2008), available at <https://datatracker.ietf.org/doc/html/rfc5322#appendix-A.1>.

⁴ Resnick, P., “Internet Message Format”, RFC 5322 – Appendix A-2, Network Working Group, Qualcomm Incorp. (2008), available at <https://datatracker.ietf.org/doc/html/rfc5322#appendix-A.2>.

```

-----
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
So, "Hello".
-----

When sending replies, the Subject field is often retained, though
prepended with "Re: " as described in section 3.6.5.

-----
From: Mary Smith <mary@example.net>
To: John Doe <jdoe@machine.example>
Reply-To: "Mary Smith: Personal Account" <smith@home.example>
Subject: Re: Saying Hello
Date: Fri, 21 Nov 1997 10:01:10 -0600
Message-ID: <3456@example.net>
In-Reply-To: <1234@local.machine.example>
References: <1234@local.machine.example>

This is a reply to your hello.
-----

Note the "Reply-To:" field in the above message. When John replies
to Mary's message above, the reply should go to the address in the
"Reply-To:" field instead of the address in the "From:" field.
-----

-----
To: "Mary Smith: Personal Account" <smith@home.example>
From: John Doe <jdoe@machine.example>
Subject: Re: Saying Hello
Date: Fri, 21 Nov 1997 11:00:00 -0600
Message-ID: <abcd.1234@local.machine.test>
In-Reply-To: <3456@example.net>
References: <1234@local.machine.example> <3456@example.net>

This is a reply to your reply.
-----

```

31. SMTP traces its origins back to the early 1980s and was initially defined in RFC 821.⁵ Because RFC 821 was primarily concerned with internal communications between networks during the infancy of the Internet, “SMTP, by default, has no mechanism for authentication and does not provide any security or privacy to email communication.”⁶ Because

⁵ J. Postel, “Simple Mail Transfer Protocol,” RFC 821 (1982), available at <https://datatracker.ietf.org/doc/html/rfc821>.

⁶ Sheikh at 117.

of this, “the communication between SMTP servers and clients occurs using plain text over unencrypted channels. Over an untrusted network, the email communication can be subjected to an eaves dropping attack without much effort.”⁷ Moreover, conventional SMTP protocols do not scale well when applied to mass email communications.

32. Even with the addition of security and privacy features that have been added by SMTP extensions⁸, “[e]mail SPAM or unwanted email is one of the major problems in the email communication system in contemporary times and does not have any fully functional permanent solutions.”⁹

33. For example, “[m]alicious mass-mailing activity on the Internet is a serious and continuing threat that includes mass-mailing worms, spam, and phishing.”¹⁰ It was also well-known that “Internet users [we]re inundated by a steady stream of emails infected with malicious code (mass-mailing worms and viruses), unwanted product advertisements (spam), and requests for personal information from criminals masquerading as legitimate entities to enable the commission of fraudulent activity (phishing).”¹¹ It was also well-known that email SPAM and other unwanted email may result in data breaches.

34. “Modern consumers frequently have become the victims of data breaches, data misuse and other events that compromise their privacy on the Internet.” ’107 Patent, 2:59-61. In just the first six months of 2019, there were more than 3,800 publicly disclosed breaches

⁷ *Id.*

⁸ *Id.*; see also J. Klensin, “Simple mail transfer protocol,” RFC 5321 (2008), available at <https://tools.ietf.org/html/rfc5321>.

⁹ Sheikh at 117.

¹⁰ Whyte, D., et al., *Addressing Malicious SMTP-based Mass-Mailing Activity Within an Enterprise Network*, 22nd Annual Computer Security Applications Conference, at 1 (Dec. 2006), available at <https://people.scs.carleton.ca/~kranakis/Papers/whytemassmailtech.pdf>.

¹¹ *Id.*

exposing 4.1 billion compromised records, approximately 70% of which exposed a person's email address.¹²

35. “However, it is rarely an option for a consumer (e.g., an end user) not to give out her personal information such as email information, name, phone number etc., and still conduct most any transaction in today's information centric economy. Such transactions including, but not limited to, ordering goods and services on-line, communicating with merchants, employers, government, friends, acquaintances and others etc., would be very difficult and inconvenient without such disclosure.” ’107 Patent, 2:61-3:2.

36. SMTP's lack of security and privacy features also presents significant problems with email chain threading. “Email chain threading” refers to the series or “chain” of email messages comprised of the original message, replies, and forwarded messages. Without security and privacy features, an end user's private information, such as her email address, is exposed to the relying party, further increasing the risk of the end user becoming a victim of a data breach or data misuse.

37. Thus, the state of the art lacked sufficient means for allowing end users to communicate by email with others and maintain email chain threading without disclosing their personal information, including but not limited to, email addresses.

38. Accordingly, there was a significant need for tools to efficiently protect privacy of end users and others over the Internet while still allowing for full and robust communication by email.

¹² D. Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, Forbes (Aug. 20, 2019), available at <https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=113a5f8bbd54>.

**AUTOGRAPH INC. AND THE DEVELOPMENT OF THE PATENTED
TECHNOLOGIES**

39. The innovations in the '107 Patent began with inventor Brian Roundtree.

40. In or around early 2010, Mr. Roundtree founded autoGraph Inc. ("AutoGraph" or "the Company"). Its initial core business mission was to solve privacy issues around advertising while improving advertising performance. AutoGraph's first product focused on allowing users to express their personal preferences without Personally Identifiable Information (PII).

41. AutoGraph provided advertisers access to people's personal preferences so businesses could better serve their customers. As it deployed the service, AutoGraph found that its customers would buy its services because it improved advertisement performance, but in their internal systems, they wanted to link to and access users' PII. This exposed a dilemma that went against AutoGraph's core mission. This led to AutoGraph focusing on how to allow users to exercise better control over how their personal preferences and PII are accessed and used by others.

42. In 2013, AutoGraph began focusing on solving the problem of how users could allow various entities to use their PII without having direct access to it. AutoGraph then developed a series of products (and obtained related patents) around the general problem of user-controlled access to personal data and PII without losing control of the data itself. AutoGraph referred to its inventive products and processes as "Data Cloaking."

43. The following links are exemplary of AutoGraph's use of its cloaking and decloaking technology:

YouTube Explainer Video published July 2019: <https://youtu.be/BdTLAqz7mC4>

autoGraph website in WebArchive:

<https://web.archive.org/web/20200313194412/https://www.autograph.me/>

44. Using Data Cloaking, users could provide single-use tokens that would allow various entities, like businesses, to use their PII without direct access to their PII. Businesses could submit these user tokens and answer questions or perform tasks like sending email, shipping a package, or making a voice call, without having their real email address, knowing their real home address, or knowing their real phone number.

45. AutoGraph continued developing supporting technologies. To provide a more personalized experience, AutoGraph developed and launched its email cloaking technology at least as early as May 2019, and continued to develop further improvements, which was referred to as “Email Cloaking.”

46. Email Cloaking is a technology directed to inhibiting the ability of businesses and fraudsters to use people’s email addresses to link them across the internet and track their activities and interests using their permanent email addresses. As described by Roundtree in 2019, “[w]e recognized as we built Personal Data Cloaking that just being anonymous would end up creating a poor customer experience; hence the self-profiling capability we have built into Personal Data Cloaking. Now personalization is based on what you actually want instead of having your online identity being tracked.”¹³

THE PATENT-IN-SUIT

47. On June 14, 2022, the ’107 Patent, titled “Privacy Friendly Communication by Operation of Cloaked/Decloaked Email,” was duly and legally issued by the United States Patent and Trademark Office (“USPTO”) to Rally, Inc., with Brian Roundtree as named inventor, and Rally AG LLC as assignee. A copy of the ’107 Patent is attached hereto as **Exhibit A**.

¹³ *autoGraph Launches Personal Data Cloaking*, PR Newswire (July 2, 2019), available at <https://www.prnewswire.com/news-releases/autograph-launches-personal-data-cloaking-300879202.html>.

48. The '107 Patent originally was assigned to AutoGraph by its inventor, Brian Roundtree. AutoGraph subsequently transferred ownership of the '107 Patent to Rally, and Rally is the current owner of all rights, titles, and interests in and to the '107 Patent.

49. Plaintiff is the owner of the entire right, title, and interest in and to the '107 Patent, including the right to sue for and collect past, present, and future damages and to seek and obtain injunctive or any other relief for infringement of the '107 Patent.

50. AutoGraph's Email Cloaking technology is the subject of the '107 Patent.

51. The '107 Patent generally relates to protecting privacy of end users and others on the Internet when communicating with others through SMTP-based computer network email systems in a manner that deviates from standard SMTP protocols while still presenting the end user with the look and feel of typical email communication via SMTP protocols.

52. In other words, the '107 Patent is directed to a technologically improved environment that is unique to SMTP-based computer network email communications. In this environment, it is rarely an option for consumers not to give out their personal information such as email information, name, phone number etc., and still conduct a transaction in today's information centric economy.

53. The '107 Patent specifies how interactions within a specific SMTP-based email computer environment are manipulated to yield a desired result – a result that overrides the routine and conventional sequence of events described in the SMTP protocol that are ordinarily triggered by the sending of an email involving a third party.

54. Specifically, the '107 Patent discloses tools to enable an end user's device to communicate via email with others such as relying-parties (e.g., merchants, third parties, etc.) without revealing their information to the relying-party such as their email address, name, or any

other information they desire to keep confidential while still being able to have commercially useful transactions with the relying parties and others.

55. For example (and by way of example only), in one embodiment, the '107 Patent and Claim 13 itself demonstrate that the claim encompass patent eligible subject matter specific to the email technological environment as shown Claim 13.

56. Claim 13 of the '107 Patent recites “[a] non-transitory computer readable medium for a ID cloaking system” that executes instructions to:

- receive an email addressed to a cloaked end user address, wherein the email is sent from a relying party email address, and wherein the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain;

- identify an end user specified address associated to the cloaked end user address by an end user profile;

- determine whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address, wherein the relying party address has a different domain than the cloaked relying party email address;

- where the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address, then generate a new cloaked relying party email address and associate the new cloaked relying party email address to the end user profile, the cloaked end user address, wherein the new cloaked relying party email address is generated with a domain different than the relying party address; and

- send the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address.

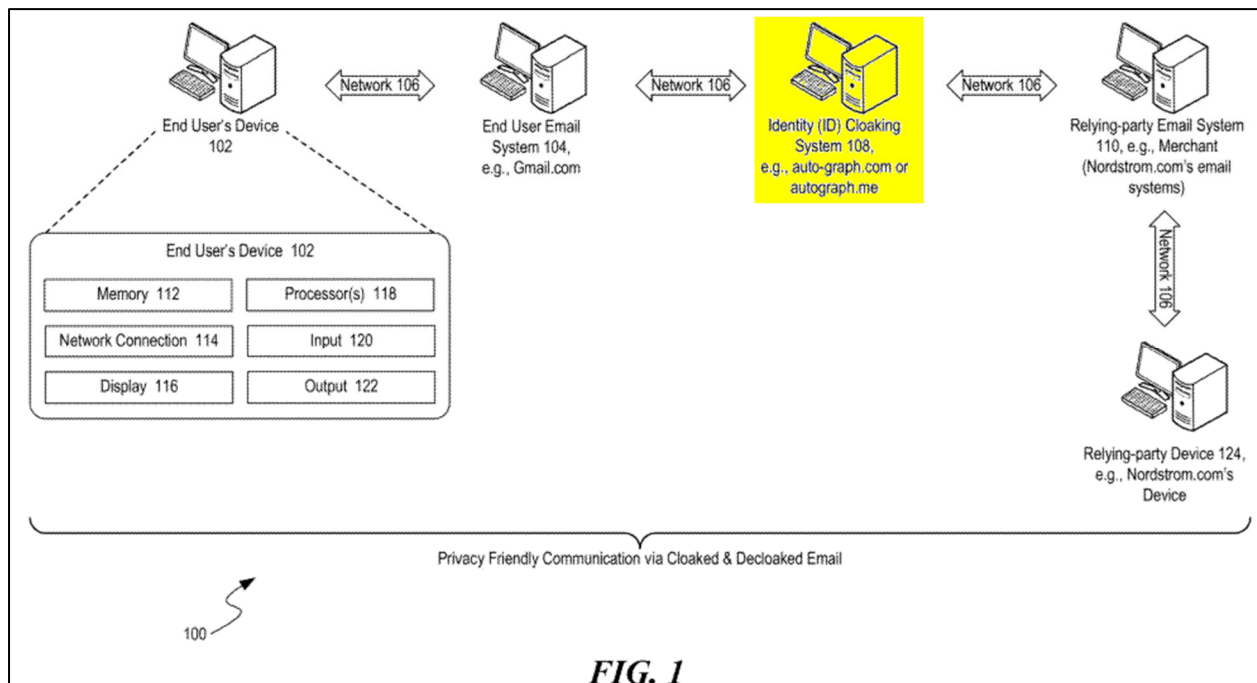
57. For example (and by way of example only), in one embodiment, the '107 Patent shows that the claim encompass patent eligible subject matter specific to the email technological environment as shown in at least the following limitations from Claim 13:

- wherein *the domain of the cloaked end user address* and *the domain associated to the cloaked ID system* are the same domain,
- wherein *the new cloaked relying party email address* is generated with *a domain different than the relying party address*, and
- wherein *the email* is configured with *a reply-to email address* comprising *the new cloaked relying party email address*.

58. Unlike conventional SMTP email processing and formatting (as shown above), for example, the ID cloaking system of the '107 Patent requires an email configured with a reply-to email address comprising the new cloaked relying party email address. This processing occurs within a two-domain SMTP-based computer environment.

59. Unlike conventional SMTP email processing and formatting (as shown above), for example, the '107 Patent identifies two different domains that exist within which an artificially generated email address is used to cloak or hide the user's identity from a third party.

60. Moreover, unlike conventional SMTP email processing and formatting, the ID cloaking system 108 “serves as an intermediary between the end user’s email system and the relying-party’s email system” to “protect[] privacy by cloaking and de-cloaking confidential information in emails as they travel between these parties . . . without the need to [also] modify the end user email system 104 or the relying party email system 110” operating under conventional SMTP protocols. ’107 Patent, 4:5-13, 4:53-54; *see also id.* at Fig. 1 (reproduced below, highlighting added).



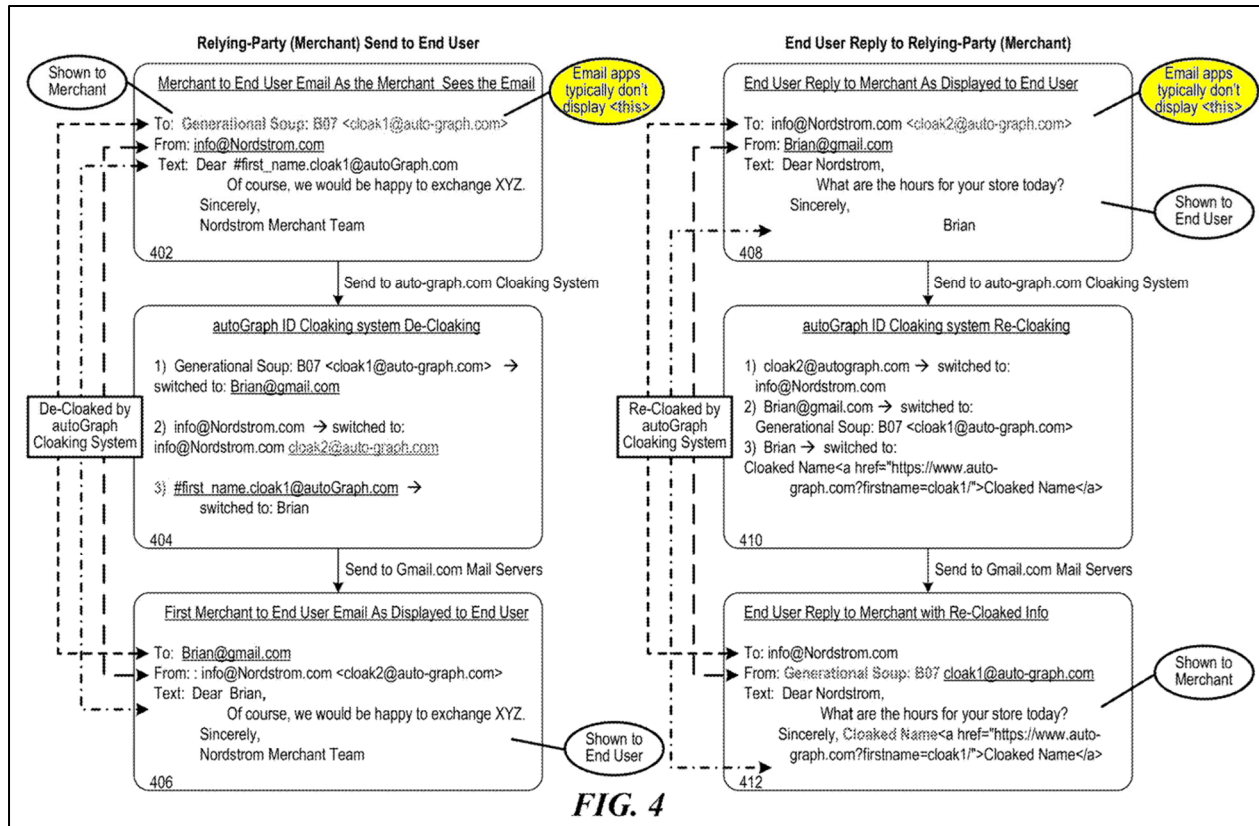
61. “The ID cloaking system maintains its status/function as an intermediary between the email servers by operation of intelligently interchanging/swapping/replacing “to” and ‘from’, ‘reply-to’ email addresses on emails as well as other information depending on which recipient the email is addressed to (the actual intended recipient). In this manner, any emails exchanged between the end user and relying-party will be delivered first to the ID cloaking system before being delivered to the other party for re-rerouting and privacy processing.” ’107 Patent, 4:65-5:7.

62. Further, the particular elements of Claim 13, considered both individually and as an ordered combination, transform the nature of the claim into a patent-eligible application as shown by at least the following limitations from Claim 13 requiring an unconventional manipulation of end user and relying party email addresses that deviates from conventional SMTP protocols:

- wherein the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain,
- wherein the new cloaked relying party email address is generated with a domain different than the relying party address, and
- wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address.

63. Unlike conventional SMTP email processing, by requiring that “the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain,” the ’107 Patent maintains the end user’s confidential and personal information by ensuring that the end user’s email is routed through the intermediate cloaked ID system before reaching the relying party.

64. Unlike conventional SMTP email processing and by requiring that “the new cloaked relying party email address is generated with a domain different than the relying party address,” the ’107 Patent maintains the end user’s confidential and personal information by ensuring that the relying party’s email is routed through the intermediate cloaked ID system before reaching the end user. *See* ’107 Patent, Fig. 4 (reproduced below, highlighting added).



65. Unlike conventional SMTP email processing and by requiring that “the email is configured with a reply-to email address comprising the new cloaked relying party email address,” the ’107 Patent enables emails exchanged between the end user and relying party to maintain email chain threading. Specifically, email chain threading is accomplished in an unconventional manner, for example, by the “intelligent assignment of the de-cloaking & cloaking addresses.” ’107 Patent, 5:8-11. “This intelligent assignment of the de-cloaking & cloaking addresses helps maintain email threading by keeping the ID cloaking system as an intermediary during the email correspondence between the end user and relying-party.” *Id.*

66. This unconventional manner of email chain threading provides the benefit of not only keeping the cloaking system as an intermediary, but also protecting the end user’s privacy and allowing deployment of the disclosed tools without the need to modify the end user’s

email system or third party's email system. "This is because the ID cloaking system's intelligent assignment of the cloaked address and de-cloaking addresses associated to the end user and relying-party leverage the SMTP routing that is used to route emails for delivery to an intermediate such as the ID Cloaking System 108 (e.g., ID cloaking system may assign email addresses to the same domain the ID cloaking system is associated to, such as autograph.me. This ensures delivery back to the ID cloaking system." '107 Patent, 5:36-44.

67. In this unconventional manner of email chain threading, the communication between the end user and relying party happens transparently given neither the end user nor the merchant/relying party must type in new email addresses, *i.e.*, they only need "reply" to existing emails. By following the unconventional series of steps but by still maintaining the look and feel of an email chain, the user is not only able to operate the system as she usually would, but the chain provides necessary context to the communication and helps remind the user of what the communication is about. As such, the end user's sensitive information (even her real email address) never falls into the hands of the merchants or others whose use of the information may be trusted but still are susceptible to data breaches. '107 Patent, 4:55-62.

68. Moreover, it was not conventional, routine, or well-known in the art to combine the above-described limitations of Claim 13 in this unique way to simultaneously provide end user anonymity, maintain email threading across different domains, and prevent SPAM emails.

69. To illustrate this further, Defendant itself has sought and received approval of a remarkably similar (if not identical subject matter which can be seen in Defendant's published application US20200382455A1 ("Defendant's Application" – Exhibit B hereto) which claims subject matter that is *strikingly similar* to the subject matter of Claim 13 of the '107 patent. Defendant's Application was filed *after* the priority date of the '107 Patent. Defendant's

Application is directed to systems and methods of an anonymous email relay. Specifically, the subject matter of Defendant's Application provides for end user anonymity by cloaking the end user's email address.

70. During prosecution at the U.S. Patent Office, Defendant's Application received a rejection for claiming non-patentable subject matter under Section 101. (*See* U.S. Patent Office's Office Action dated November 6, 2023). (Exhibit C hereto). Defendant overcame that Section 101 rejection by inserting one word, "non-transitory" into the preamble of the pending claims.; (*See* Defendant's Office Action Response dated January 31, 2024). (Exhibit D hereto). In response, the U.S. Patent Office allowed the claims of Defendant's Application based upon that amendment. (*See* U.S. Patent Office's Notice of Allowance dated March 6, 2024). (Exhibit E hereto).

71. In allowing Defendant's Application, the U.S. Patent Office deemed the claims in Defendant's Application not to be conventional, routine, or well-known in the art. Accordingly, this allowance further illustrates that the strikingly similar subject matter of Claim 13 is also not conventional, routine, or well-known in the art. (It is noted that Claim 13 of the '107 Patent also contains the word "non-transitory.")

72. Accordingly, the "inventive concept" of the '107 Patent involves non-routine and unconventional processing that is not found in the industry.

COUNT I
INFRINGEMENT OF THE '107 PATENT

73. Plaintiff repeats and realleges the above paragraphs, which are incorporated by reference as if fully restated herein.

74. Plaintiff is the owner of all rights, title, and interest in the '107 Patent and, at a minimum, all substantial rights in the '107 Patent, including the exclusive right to enforce

the patent and all rights to pursue damages, injunctive relief, and all other available remedies for past, current, and future infringement.

75. Plaintiff and its predecessors in interest have never licensed the Defendant under the '107 Patent, nor has Plaintiff otherwise authorized the Defendant to practice any part of the '107 Patent.

76. The '107 Patent is presumed valid under 35 U.S.C. § 282.

77. Defendant operates, provides, and controls systems and methods that cloak and decloak emails.

78. On information and belief, Defendant, alone and/or jointly in conjunction with employees, agents, and/or customers under its control, has directly and/or indirectly infringed and continues to directly and/or indirectly infringe the '107 Patent pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, by using SMTP-based computerized methods and systems for cloaking and decloaking email messages that are covered by one or more claims of the '107 Patent, including Claim 13 of the '107 Patent, without license or authority.

79. For example, as shown in paragraphs 80 to 90 below, the Accused Products and their infringing activities utilize applications operated or licensed by Defendant that enable, contribute to, and induce its customers and users to cloak and decloak messages. These paragraphs refer to two instructional Hide-My-Email videos published on-line. The first video is entitled “How To Use [Apple’s] Hide My Email On Mac and iPhone” and is located at https://www.youtube.com/watch?v=EFsoN_Au_-Q (the “First Hide-My-Email Video”). The second video is entitled “How to use [Apple’s] Hide My Email with iCloud” and is located at <https://www.youtube.com/watch?v=oJRrkJy0vUk> (the “Second Hide-My-Email Video”). Further details of this product provided by Defendant also are published by Defendant on its own web

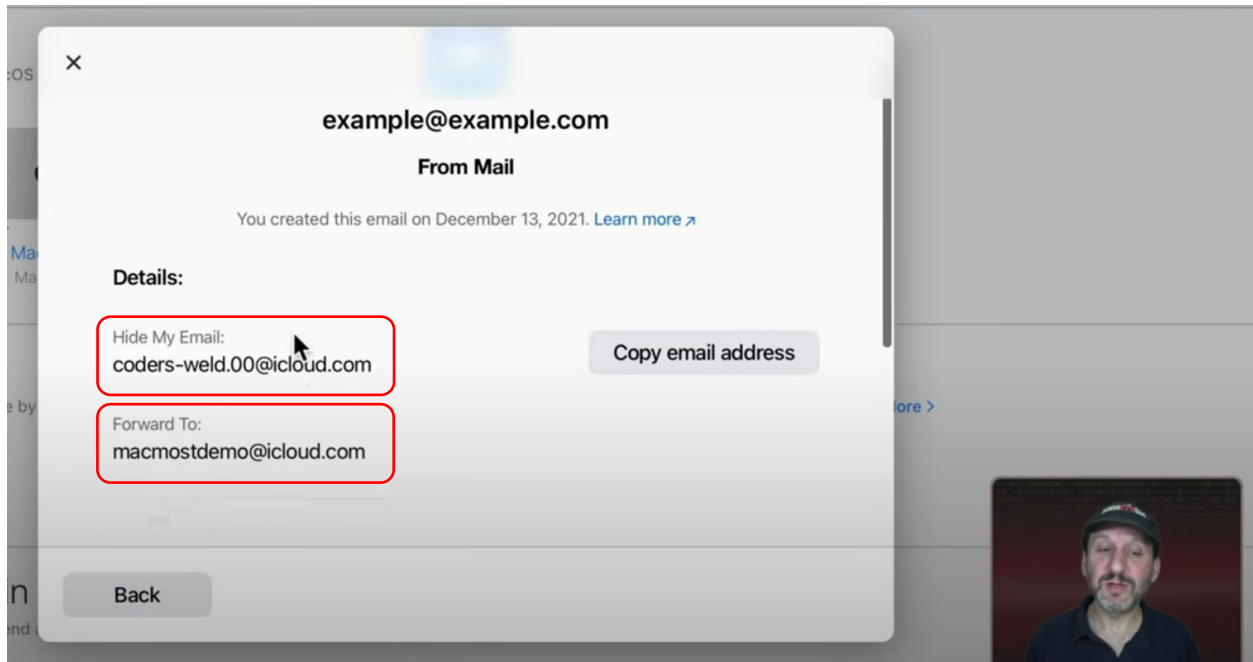
page located at www.support.apple.com/en-us/105078, which provides details titled “How Hide My Email works.”

80. On information and belief, the Accused Products provide “[a] non-transitory computer readable medium for a ID cloaking system” by operating the website <https://www.Apple.com/> and providing a mobile application in order to provide privacy measures to its customers and users, including but not limited to its “Hide-My-Email” feature.

81. On information and belief, the Accused Products “receive an email addressed to a cloaked end user address, wherein the email is sent from a relying party email address.” For example, according to Defendant, the “Hide-My-Email” product “lets you create unique, random email addresses that forward to your personal inbox so you can send and receive email without having to share your real email address.”

82. On information and belief, the Accused Products provide that “the domain of the cloaked end user address and the domain associated to the cloaked ID system are the same domain.” For example, according to Defendant, the “Hide-My-Email” product routes end user and relying party emails through the same intermediary computer system located at the same domain (i.e., iCloud.com).

83. On information and belief, the Accused Products “identify an end user specified address associated to the cloaked end user address by an end user profile” as shown in the following screen shot from the First Hide-My-Email Video.

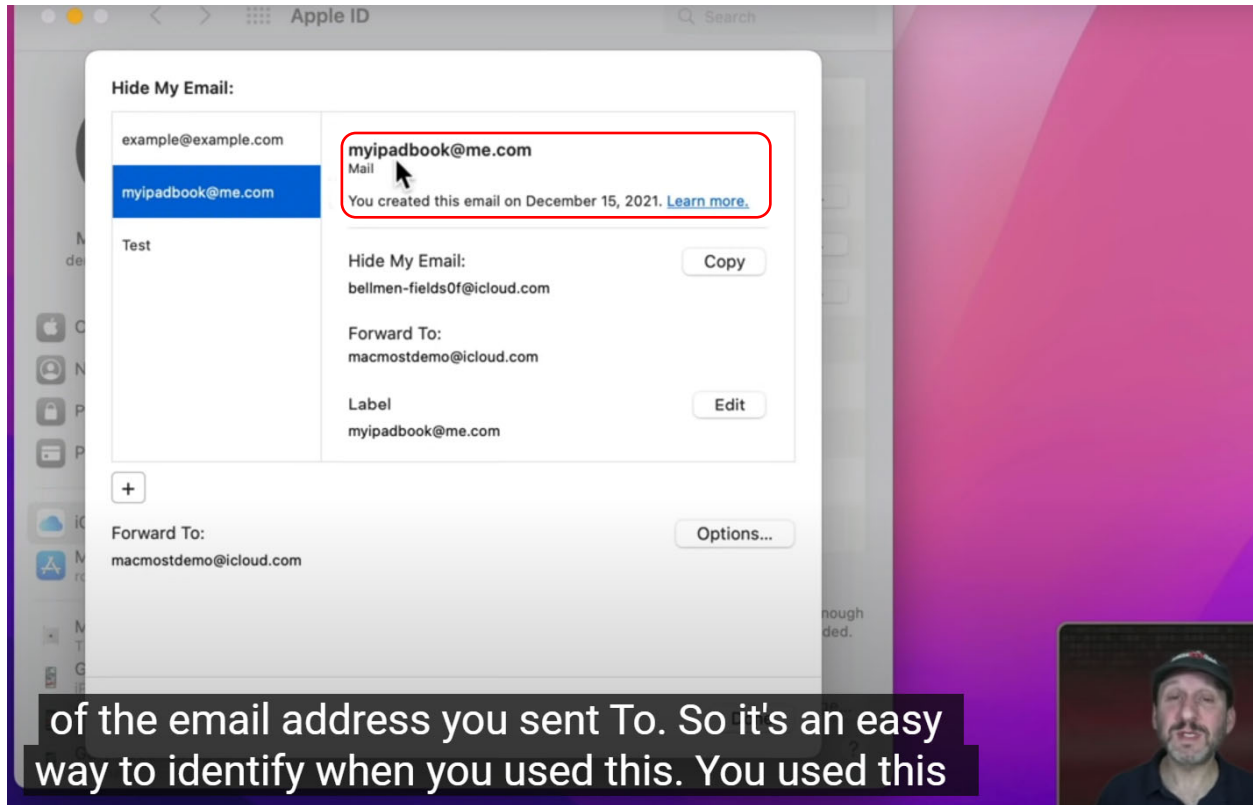


First Hide-My-Email Video at time stamp 6:21/11:44 (red outlining added).

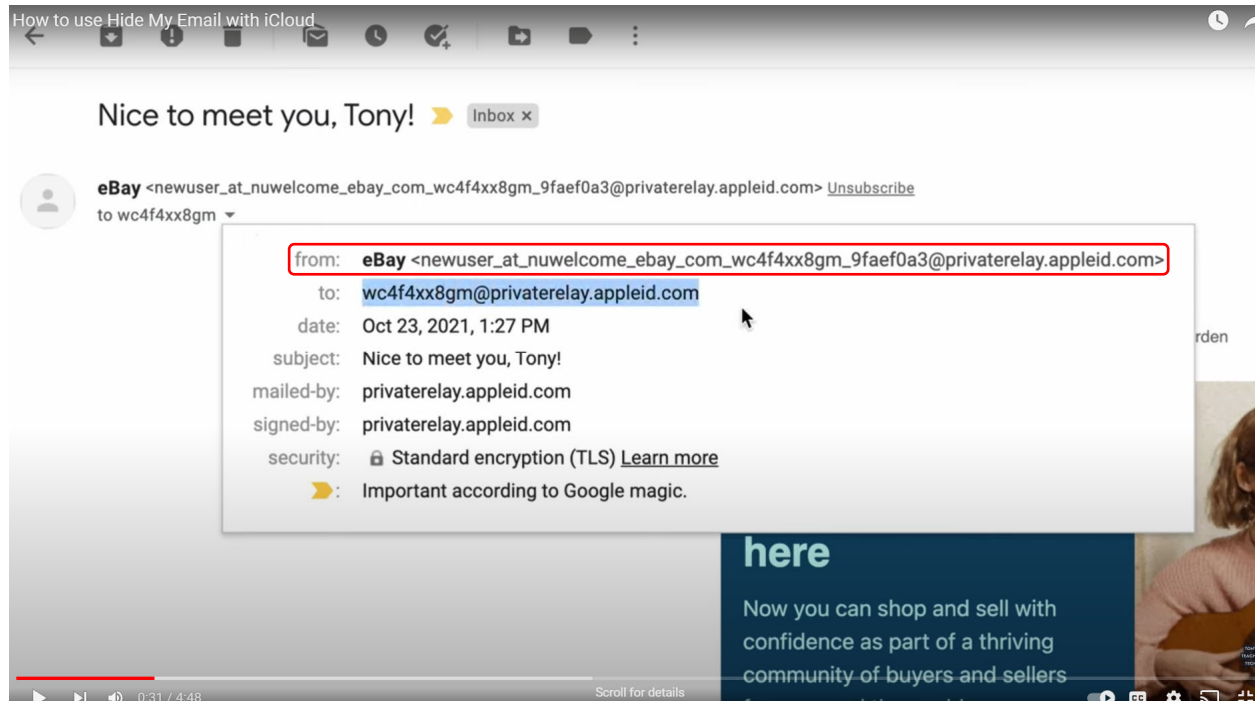
84. In the above example, the cloaked end user email address (under the “Hide My Email” field) is “coders-weld.00@icloud.com” and the actual end user email address (under the “Forward To” field) is “macmostdemo@icloud.com”

85. On information and belief, the Accused Products “determine whether the end user profile contains a previous association between the relying party address and a cloaked relying party email address, wherein the relying party address has a different domain than the cloaked relying party email address” as shown by the first screenshot from the First Hide-My-Email Video and the second screenshot from the Second Hide-My-Email Video. The first screenshot below shows the relying party address as “myipadbook@me.com,” the cloaked end user email address as “bellmen-fields0f@icloud.com,” and the end user email address as “macmostdemo@icloud.com.” The second screenshot below shows a relying party email address and its associated cloaked relying party email address are persistent through email exchanges (where the relying party is “eBay,” the cloaked relying party email address is

newuser_at_nuwelcome_ebay_com_wc4f4xx8gm_9faef0a3@privaterelay.appleid.com). The relying party address (“eBay.com”) has a different domain than the cloaked relying party email address (“privaterelay.appleid.com”).



First Hide-My-Email Video at time stamp 7:32/1:44 (red outlining added).

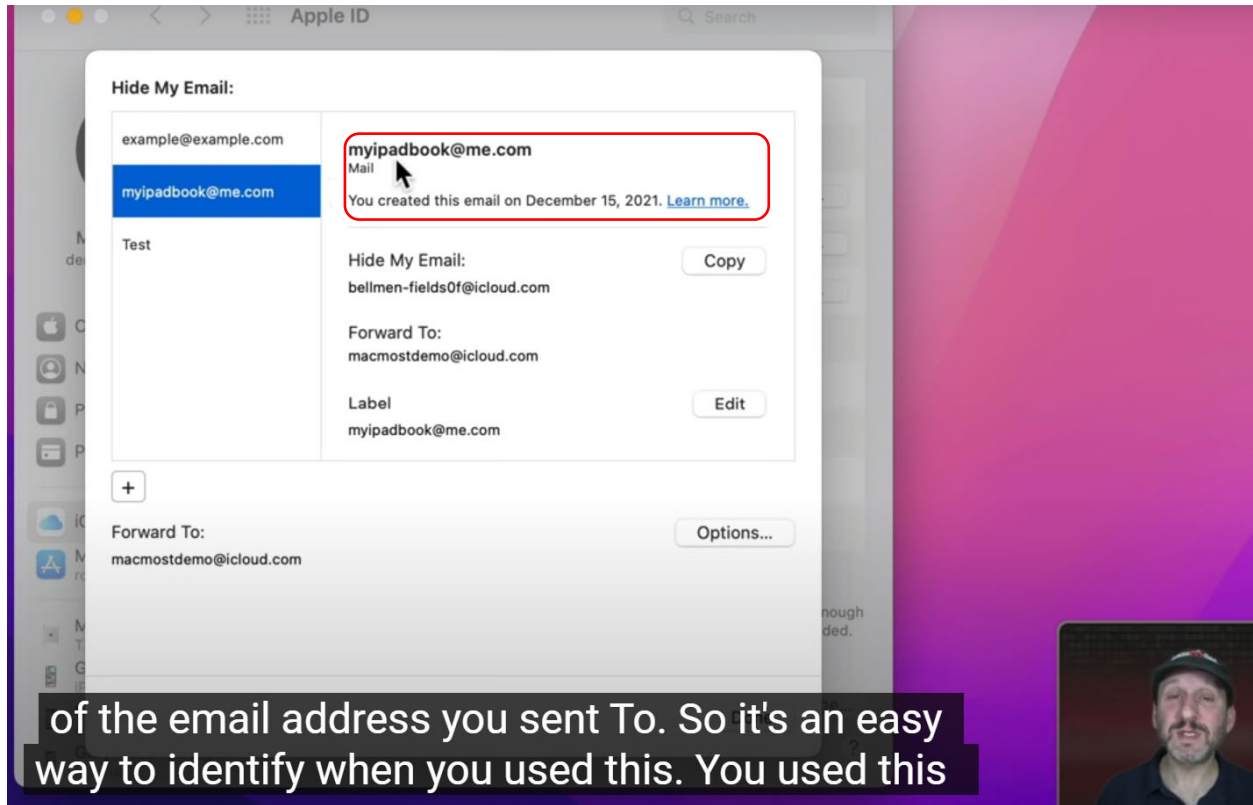


Second Hide-My-Email Video at time stamp 0:27/4:48 (red outlining added).

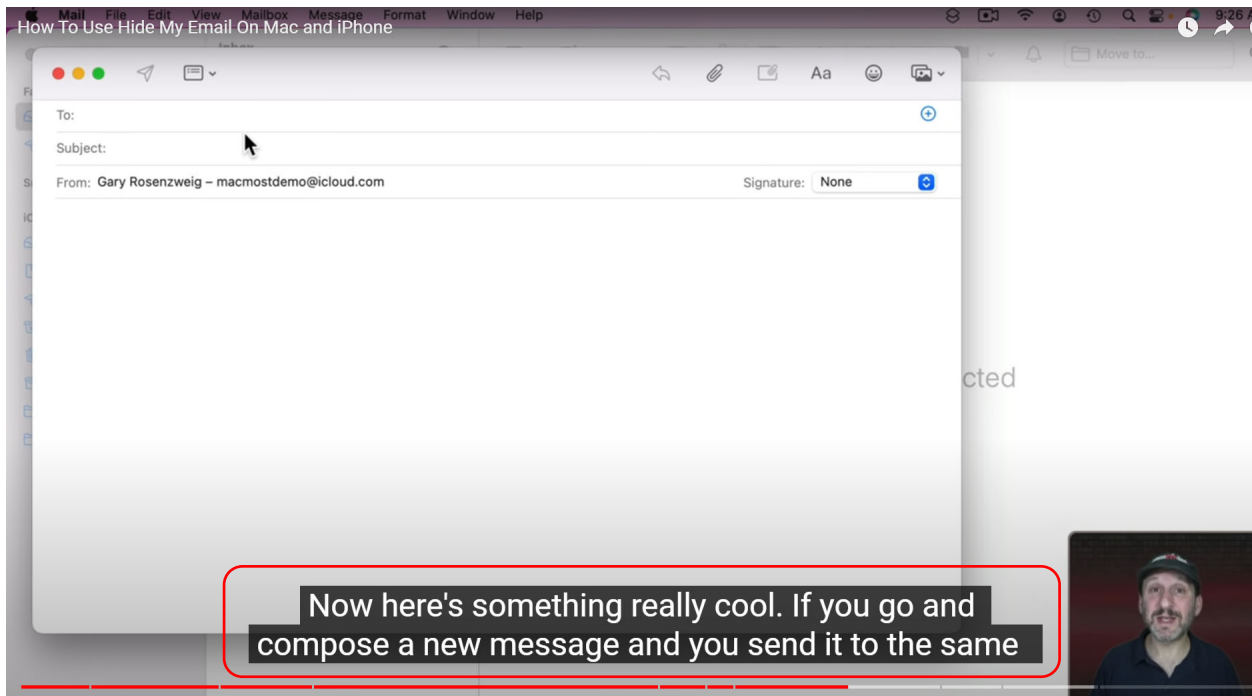
86. On information and belief, the Accused Products provide that “where the end user profile does not contain a previous association between the relying party address and the cloaked relying party email address, then generate a new cloaked relying party email address and associate the new cloaked relying party email address to the end user profile, the cloaked end user address, wherein the new cloaked relying party email address is generated with a domain different than the relying party address” as shown by the following screenshot from the First Hide-My-Email Video. The sequence of exemplary screenshots from the First Hide-My-Email Video below shows that the cloaked relying party email address is persistent throughout the email exchanges between the end user and the relying party, and a new cloaked relying party email address is generated with a different domain and associated to the end user profile’s information (e.g., hide-my-email address, etc.). The dialogue from the First Hide-My-Email Video is as follows:

“Now here’s something really cool. If you go and compose a new message and you send it to the same person and you choose Hide My Email, instead of creating a new one it’s

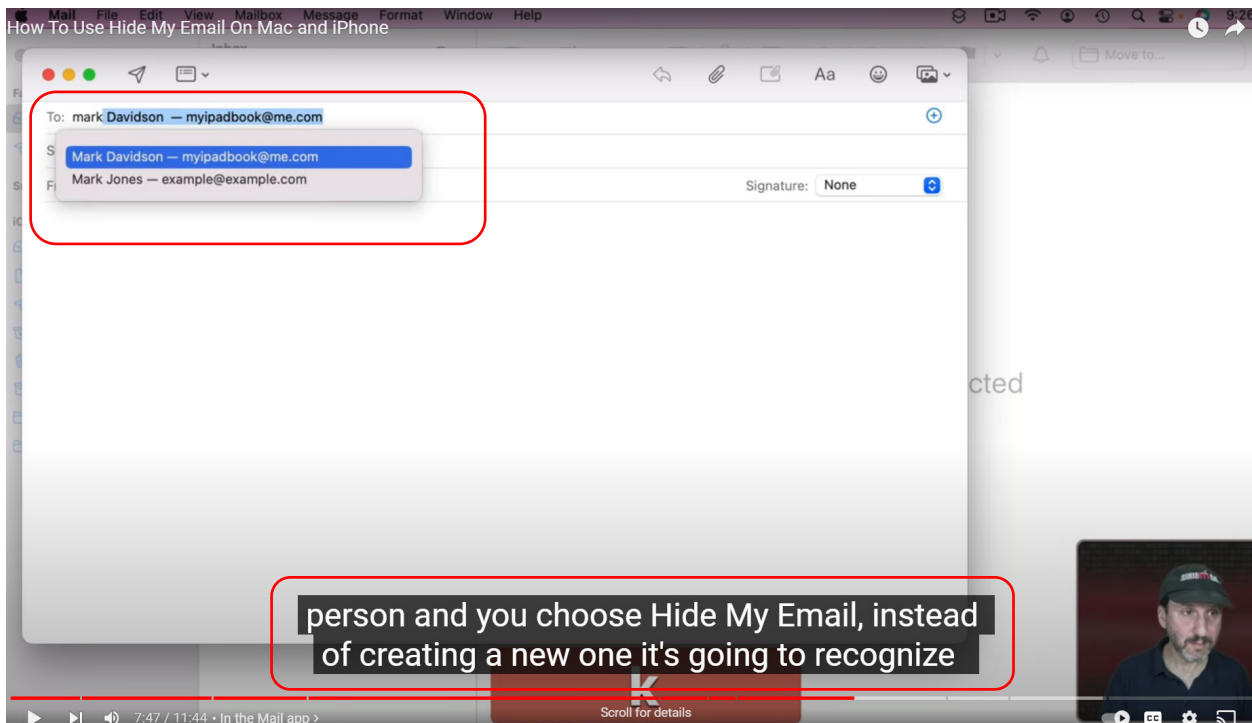
going to recognize that you're sending to a person that you already used a special email address for and it's going to reuse that same one. So that person will see that same special email address for you. It's not going to create a new one each and every time. This allows you to correspond back and forth with the same person and always use that special email address."



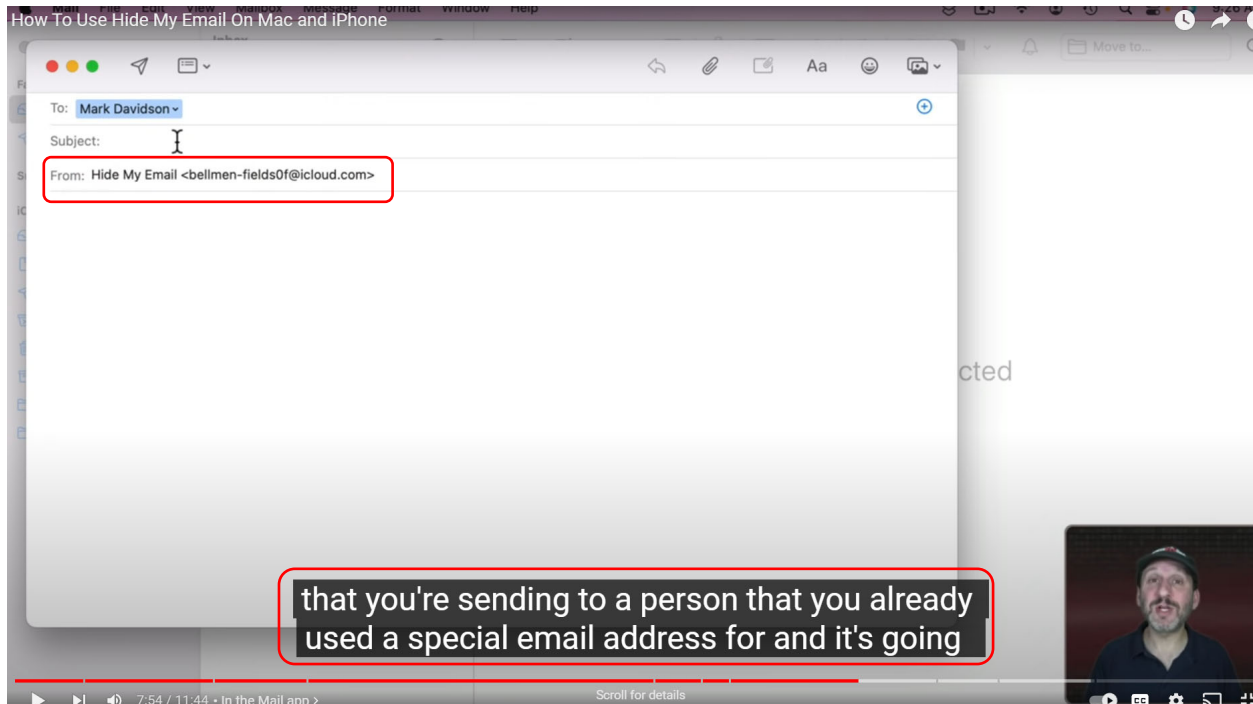
First Hide-My-Email Video at time stamp 7:32/11:44 (red outlining added).



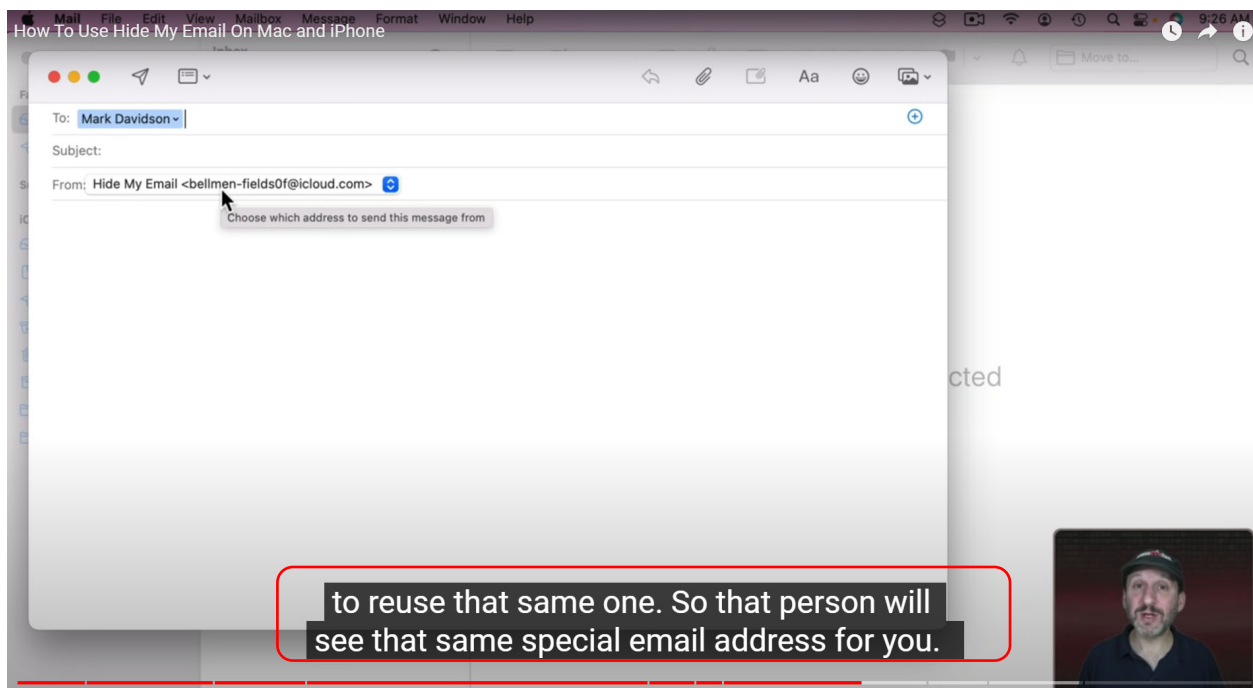
First Hide-My-Email Video at time stamp 7:44/11:44 (red outlining added).



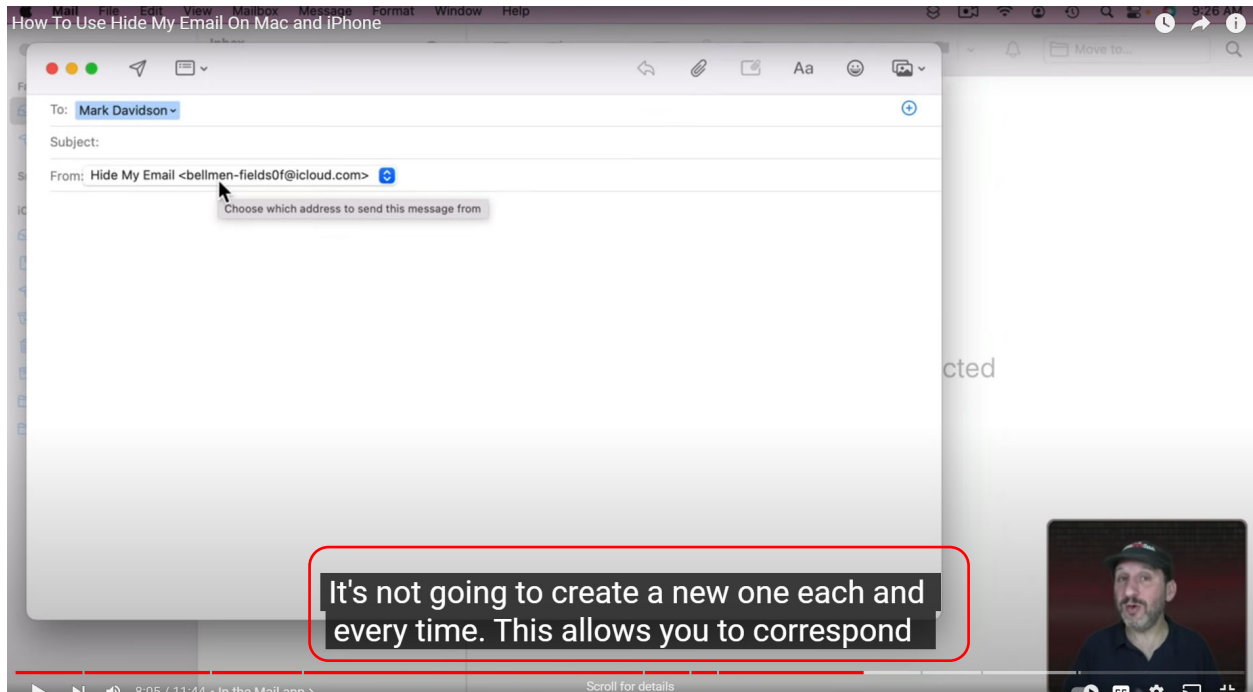
First Hide-My-Email Video at time stamp 7:47/11:44 (red outlining added).



First Hide-My-Email Video at time stamp 7:54/11:44 (red outlining added).



First Hide-My-Email Video at time stamp 7:59/11:44 (red outlining added).

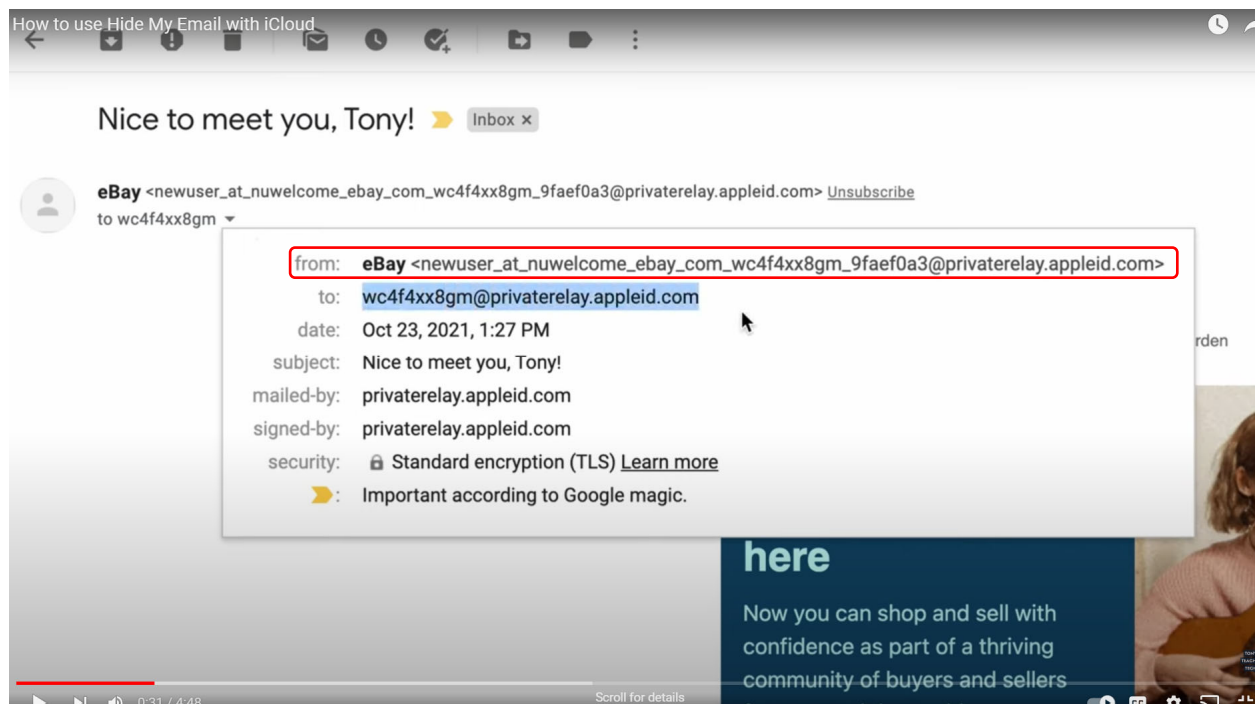


First Hide-My-Email Video at time stamp 8:03/11:44 (red outlining added).



First Hide-My-Email Video at time stamp 8:09/11:44 (red outlining added).

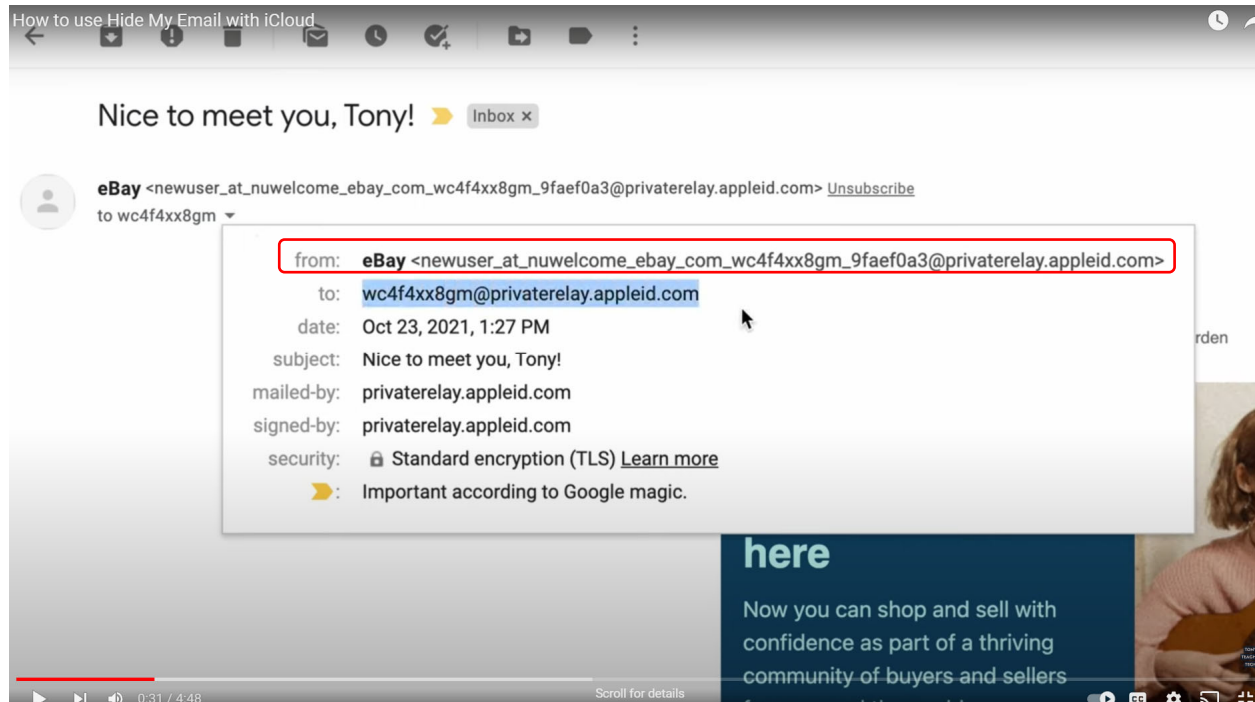
87. On information and belief, the exemplary screenshot below from the Second Hide-My-Email Video shows that a relying party email address and its associated to cloaked relying party email address are persistent throughout email exchanges (where the relying party is “eBay,” the cloaked relying party email address is newuser_at_nuwelcome_ebay_com_wc4f4xx8gm_9faef0a3@privaterelay.appleid.com). The relying party address (“eBay.com”) has a different domain than the cloaked relying party email address (“privaterelay.appleid.com”).



Second Hide-My-Email Video at time stamp 0:27/4:48 (red outlining added).

88. On information and belief, the Accused Products “send the email to the identified end user specified address, wherein the email is configured with a reply-to email address comprising the new cloaked relying party email address” as shown by the following screenshot from the Second Hide-My-Email Video. In the exemplary screenshot below, the email shows the relying party “eBay” with its “reply to” portion configured with the new cloaked relying party address

“newuser_at_nuwelcome_ebay_com_wc4f4xx8gm_9faef0a3@privaterelay.appleid.com.” Upon information and belief, when the end user “Tony” replies to this email, the reply-to email address includes the new cloaked relying party email address.



Second Hide-My-Email Video at time stamp 0:27/4:48 (red outlining added).

89. These activities infringe at least Claim 13 of the '107 Patent as reproduced above.

90. To the extent that the claims of the '107 Patent may be construed prior to the claim construction process or discovery, such construction must be that which is most favorable to Plaintiff. Plaintiff's allegations support a plausible claim construction detailing a reliable and secure method for protecting an end user's privacy in an SMTP-based email network, distinct from passing notes through an intermediary or anonymous remailers.

91. This Court must take Plaintiff's factual allegations in its Complaint, including those mapping the claims of the '107 Patent to Defendant's infringing activities, as true

in determining the sufficiency of Plaintiff's complaint under Federal Rule of Procedure 12 or the eligibility of the '107 Patent under 35 U.S.C. § 101.

92. As a result of Defendant's infringement of the '107 Patent, Plaintiff has suffered monetary damages in an amount yet to be determined and will continue to suffer damages in the future. Defendant is liable to Plaintiff for such damages, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

93. Defendant's wrongful acts have damaged and will continue to damage Plaintiff irreparably, and Plaintiff has no adequate remedy at law for those wrongs and injuries. In addition to its actual damages, Plaintiff is entitled to a permanent injunction that restrains and enjoins Defendant and its agents, servants, and employees, and all persons acting thereunder, in concert with, or on its behalf, from infringing the '107 Patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff that Defendant has been and is infringing the '107 Patent pursuant to 35 U.S.C. §§ 271(a) and/or 271(b);

B. A permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in concert or privity with any of them from infringing any claims of the '107 Patent, with any additional compensation before imposition of such injunction to Plaintiff in an amount to be determined by the Court;

C. A judgment awarding Plaintiff all damages adequate to compensate it for Defendant's infringement of the Asserted Patent under 35 U.S.C. § 284, and in no event less than

a reasonable royalty for Defendant's acts of infringement, including all pre-judgment and post-judgment interest at the maximum rate permitted by law, and also any past damages permitted under 35 U.S.C. § 286, as a result of Defendant's infringement of any claims of the Asserted Patent;

D. A compulsory royalty going forward after trial and/or entry of final judgment if an injunction is not granted;

E. An accounting for all damages including damages between trial and entry of final judgment;

F. An assessment of costs, including reasonable attorneys' fees pursuant to 35 U.S.C. § 285, and prejudgment interest against Defendant; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to FED. R. CIV. P. 38, Plaintiff hereby demands a trial by jury on all issues so triable.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Lucinda C. Cucuzzella

OF COUNSEL:

Bruce J. Rose
MOORE & VAN ALLEN
100 North Tryon Street, Suite 4700
Charlotte, NC 28202-4003
(704) 331-1000
brucerose@mvalaw.com

Rodger D. Smith II (#3778)
Lucinda C. Cucuzzella (#3491)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
rsmith@morrisnichols.com
ccucuzzella@morrisnichols.com

Attorneys for Plaintiff

May 3, 2024

CERTIFICATE OF SERVICE

I hereby certify that on May 3, 2024, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on May 3, 2024, upon the following in the manner indicated:

David E. Moore, Esquire
Bindu A. Palapura, Esquire
Andrew M. Moshos, Esquire
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Attorneys for Defendant

VIA ELECTRONIC MAIL

Garland Stephens, Esquire
BLUE PEAK LAW GROUP LLP
3139 W Holcombe Blvd PMB 8160
Houston, TX 77025
Attorneys for Defendant

VIA ELECTRONIC MAIL

Anna Dwyer, Esquire
BLUE PEAK LAW GROUP LLP
25 W 31st St.
New York, NY 10001
Attorneys for Defendant

VIA ELECTRONIC MAIL

Robert Magee, Esquire
Jeff Risher, Esquire
BLUE PEAK LAW GROUP LLP
3790 El Camino Real, PMB 846
Palo Alto, CA 94306
Attorneys for Defendant

VIA ELECTRONIC MAIL

/s/ Lucinda C. Cucuzzella

Lucinda C. Cucuzzella (#3491)