IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND-ODESSA DIVISION

ZAPFRAUD, INC., **PLAINTIFF,** **v.** **TREND MICRO INCORPORATED,** **Defendant.**	**Case No. _____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff ZapFraud, Inc. ("ZapFraud") brings this action against Defendant Trend Micro Incorporated ("Defendant" or "Trend Micro") for infringement of ZapFraud's United States Patent Nos. 10,721,195 (the " '195 Patent," attached as Exhibit 1) and 11,595,336 (the " '336 Patent," attached as Exhibit 2), including their respective Certificates of Correction (collectively, the "Asserted Patents"), and hereby alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement. These claims arise under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*., based on Defendant's infringement of the Asserted Patents.

2. ZapFraud owns all right, title, and interest in and to the Asserted Patents including the right to sue for and recover damages for past, present, and future infringement.

3. Without authorization from ZapFraud, Defendant makes, uses, sells, offers for sale, and/or imports into the United States software, platforms, products, and services that infringe the Asserted Patents, including, individually and/or in combination, representative Trend

Micro email-security, cloud-security, threat-detection, BEC-detection, suspicious-link, warning, quarantine, reporting, and administrative systems and functionality, including Trend Micro Email Security / TrendAI Email Security, Cloud App Security, Hosted Email Security, ScanMail, InterScan Messaging Security, Deep Discovery Email Inspector, Smart Protection Complete, Trend Vision One, and related Trend Micro server-side, administrative, reporting, and security-action functionality (collectively, the "Accused Products").

PARTIES

4. ZapFraud is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 7 East 20th Street #12F, New York, NY 10003.

5. ZapFraud's patented technologies relate to electronic security systems and methods for defending against email fraud and misuse, including business email compromise ("BEC") scams.

6. The Asserted Patents were invented by Dr. Bjorn Markus Jakobsson, who is also known professionally as Dr. Markus Jakobsson. Dr. Jakobsson obtained his Ph.D. in Computer Science/Cryptography from the University of California San Diego in 1997. He is an expert in computer security, mobile security, malware detection, fraud analysis, and disruptive security, the author or co-author of more than 200 publications, and the inventor or co-inventor of more than 375 patents.

7. On information and belief, Defendant Trend Micro Incorporated is a corporation organized under the laws of California with a principal place of business at 225 East John Carpenter Freeway, Suite 1500, Irving, Texas 75062.

8. On information and belief, Trend Micro maintains places of business in Texas, including an office in this District at 11305 Alterra Parkway, Austin, Texas 78758.

9. On information and belief, Trend Micro conducts business in Texas, including in this District.

10. On information and belief, Trend Micro maintains a regular and established place of business in this District, including its Austin office at 11305 Alterra Parkway, Austin, Texas 78758. Trend Micro may be served through its registered agent as reflected in current secretary-of-state records.

11. On information and belief, Trend Micro designs, makes, manufactures, sells, offers to sell, imports, distributes, advertises, and/or uses the Accused Products in the United States, including throughout the State of Texas and this District, and introduces such Accused Products into the stream of commerce knowing and intending that they would be extensively used in the State of Texas and in this District.

12. This Court has subject-matter jurisdiction over this action for patent infringement under 28 U.S.C. §§ 1331 and 1338(a).

JURISDICTION AND VENUE

13. This Court has personal jurisdiction over Defendant under the Texas Long Arm Statute. Defendant has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Defendant would not offend traditional notions of fair play and substantial justice. Exercising jurisdiction over Defendant in this District thus comports with Due Process.

14. Defendant has purposely availed itself of the laws and protections of the United States and the State of Texas by knowingly making, using, selling, offering for sale, distributing, and/or advertising the Accused Products in Texas and this District. Defendant maintains continuous and systematic contacts within this District by selling and offering for sale products and services to customers in this District and by offering for sale products and services that are

used in this District. Defendant, directly or through subsidiaries or intermediaries, has regularly and systematically conducted and currently conducts substantial business in this District, including but not limited to: (i) making, using, offering for sale and/or selling infringing products or services in this District; (ii) purposefully and voluntarily placing one or more infringing products or services into the stream of commerce with the expectation that those products or services will be purchased and/or used by consumers in this District; and/or (iii) regularly doing or soliciting business, engaging in other persistent courses of conduct, or deriving substantial revenue from goods and services provided to individuals in Texas and in this District. Defendant has targeted the State of Texas and this District by conducting regular business therein, and has placed and continues to place infringing products into the stream of commerce through an established distribution channel with the expectation and/or knowledge that they will be purchased by consumers in the State of Texas and this District.

15. ZapFraud's claims for patent infringement arise directly from and/or relate to the above-referenced activity by Defendant.

16. Venue is proper in this District under 28 U.S.C. § 1400(b) because, on information and belief, Trend Micro has committed acts of infringement in this District and maintains a regular and established place of business in this District, including its office at 11305 Alterra Parkway, Austin, Texas 78758.

17. Venue is also proper because, on information and belief, Trend Micro has a regular and established place of business in this District, including an office at 11305 Alterra Parkway, Austin, Texas 78758.

18. On information and belief, Trend Micro maintains in this District documents, technical information, product personnel, support personnel, sales personnel, and/or other witnesses relevant to the Accused Products and the claims at issue in this case.

THE ASSERTED PATENTS

19. The ’195 Patent is entitled “Detection of Business Email Compromise” and issued on July 21, 2020. A true and correct copy of the ’195 Patent, including its Certificate of Correction, is attached hereto as Exhibit 1.

20. The application that issued as the ’336 Patent is a continuation of the application that issued as the ’195 Patent. The ’336 Patent is entitled “Detecting of Business Email Compromise” and issued on February 28, 2023. A true and correct copy of the ’336 Patent, including its Certificate of Correction, is attached hereto as Exhibit 2.

21. The Asserted Patents are related and share the same specification. The named inventor on each of the Asserted Patents is Bjorn Markus Jakobsson. ZapFraud owns by assignment the entire right, title, and interest in and to the Asserted Patents, including the right to sue for and recover damages for past, present, and future infringement.

22. As the shared specification of the Asserted Patents explains: “Business Email Compromise (BEC) is a type of scam that has increased dramatically in commonality in the recent past. In January 2015, the FBI released stats showing that between Oct. 1, 2013, and Dec. 1, 2014, some 1,198 companies reported having lost a total of $179 million in BEC scams, also known as ‘CEO fraud.’ It is likely that many companies do not report being victimized, and that the actual numbers are much higher. There therefore exists an ongoing need to protect users against such scams.” *E.g.*, ’195 Patent at 1:12–22; ’336 Patent at 1:15–23.

23. BEC scams often involve spoofed or deceptive emails that appear to come from trusted executives, vendors, or other parties, and are designed to trick recipients into transferring

funds, revealing sensitive information, or taking other harmful actions. Because such messages may appear to originate from a trusted source and may be targeted rather than mass-mailed, BEC scams can evade traditional spam-filtering techniques.

24. To defend against email fraud and misuse, including BEC scams, the Asserted Patents disclose and claim specific computer-implemented techniques for determining trust relationships, evaluating whether messages present email-security risks, and automatically performing security, reporting, warning, quarantine, proxy-link, and related actions. These techniques improve upon then-existing email-filtering approaches, including approaches that commonly focused on high-volume spam, blacklist-based screening, or other signals less suited to targeted BEC attacks.

25. As the Asserted Patents' shared specification elaborates:

> Unlike traditional phishing scams, spoofed emails used in CEO fraud schemes and related scams, such as those described above, are unlikely to set off traditional spam filters, because these are targeted phishing scams that are not mass emailed, and common spam filters rely heavily on the quantity of email of a certain type being sent. Also, the crooks behind them take the time to understand the target organization's relationships, activities, interests and travel and/or purchasing plans. This makes the scam emails look rather realistic—both to their recipients and to traditional spam filters.
>
> Traditional spam filtering is designed to detect typical spam. This is typically sent in high volume, has low open rates, and even lower response rates. It is commonly placed in the spam folder by the recipient (if not already done so by the spam filter). It commonly contains a small set of keywords, corresponding to the products that are most profitable for spammers to sell. These keywords are typically not used in non-spam email traffic. To avoid detection by spam filters, spammers commonly obfuscate messages, e.g., write V-!-@-G.R-A instead of "Viagra". This commonly helps the spammers circumvent spam filters, but the message is typically still clear to the recipient.

See e.g., '195 Patent at 3: 17–39; '336 Patent at 3: 17–39.

THE ACCUSED PRODUCTS

26. Defendant has, without ZapFraud's authority, made, used, offered to sell, sold, and/or imported into the United States, and/or instructed others regarding the use of, the Accused

Products. The Accused Products include Trend Micro email-security, cloud-security, threat-detection, BEC-detection, suspicious-link, warning, quarantine, reporting, and administrative functionality. By doing so, Defendant directly infringes, induces infringement of, and/or contributes to infringement of one or more claims of each Asserted Patent, literally and/or under the doctrine of equivalents.

27. References to the Accused Products include each accused product identified above, as well as Trend Micro systems in which two or more such products or components operate together, are centrally administered, report into a shared console, or otherwise provide integrated email-security, BEC-detection, suspicious-link, warning, quarantine, report-generation, and administrative functionality.

28. Defendant, directly or indirectly through its affiliates, subsidiaries, agents, customers, or other representatives, makes, uses, sells, and/or offers for sale the Accused Products in the United States and this District and/or imports the Accused Products into the United States.

29. Defendant has had knowledge of the Asserted Patents and ZapFraud's infringement allegations no later than service of this Complaint. On information and belief, Defendant has continued and will continue its infringing conduct after receiving such notice.

30. The allegations set forth herein are exemplary and without prejudice to infringement contentions provided pursuant to the Court's orders. By setting forth these allegations, ZapFraud does not convey or imply any particular claim construction or the precise scope of the claims. These infringement allegations are based on currently available information and a reasonable investigation of the Accused Products. ZapFraud reserves all rights, including the right to modify this description based on information obtained during discovery.

31. On information and belief, the Accused Products include a system for detection of BEC scams. For example, Trend Micro's website includes the following description of InterScan Messaging Security:[1]

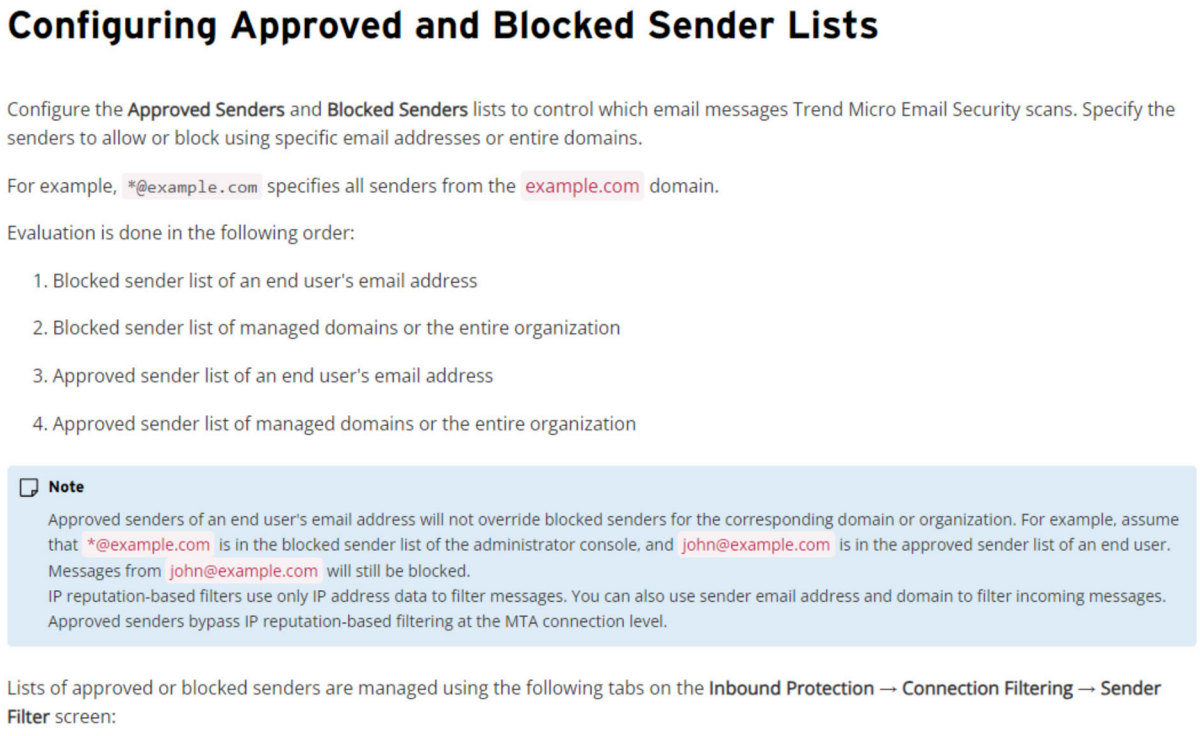
Trend Micro InterScan Messaging Security now Protects you from Business Email Compromise, Ransomware, and More [blog]

For the many medium to large size companies interested in a single vendor suite solution that features cross-solution visibility and manageability, Trend Micro™ Smart Protection Complete is an excellent choice.

32. On information and belief, the Accused Products automatically determine whether a party that may have sent a message is trusted or considered trusted by a recipient or recipient organization, including by using approved sender lists, approved domains, managed domains, organizational sender lists, allowlists/whitelists, address-book-type information, and/or historical or administrative trust relationships. For example, Trend Micro documentation describes approved and blocked sender lists that can identify allowed senders by specific email address or domain, including managed domains or entire organizations, and states that messages from approved senders are treated differently for checks including spam, BEC, phishing, social-

[1] https://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/security-strategies-for-enterprises/ent-threats-bec

engineering attack, and web-reputation filtering, such as by maintaining a whitelist as shown below.[2]



Configuring Approved and Blocked Sender Lists

Configure the **Approved Senders** and **Blocked Senders** lists to control which email messages Trend Micro Email Security scans. Specify the senders to allow or block using specific email addresses or entire domains.

For example, `*@example.com` specifies all senders from the example.com domain.

Evaluation is done in the following order:

1. Blocked sender list of an end user's email address
2. Blocked sender list of managed domains or the entire organization
3. Approved sender list of an end user's email address
4. Approved sender list of managed domains or the entire organization

Note

Approved senders of an end user's email address will not override blocked senders for the corresponding domain or organization. For example, assume that *@example.com is in the blocked sender list of the administrator console, and john@example.com is in the approved sender list of an end user. Messages from john@example.com will still be blocked.
IP reputation-based filters use only IP address data to filter messages. You can also use sender email address and domain to filter incoming messages. Approved senders bypass IP reputation-based filtering at the MTA connection level.

Lists of approved or blocked senders are managed using the following tabs on the **Inbound Protection → Connection Filtering → Sender Filter** screen:

[2] https://docs.trendmicro.com/en-us/documentation/article/trend-micro-email-security-online-help-configuring-approved

- **Approved Senders**

  Trend Micro Email Security will not perform the following checks on email messages from senders added to this list:

  - IP reputation-based filtering
  - Unknown sender domain check
  - Spam
  - BEC
  - Phishing
  - Social engineering attack
  - Web reputation
  - Graymail

  Trend Micro Email Security still performs virus scanning and content filtering on all messages received and takes the action configured in policy rules once detecting any virus or content filtering violation.

- **Blocked Senders**

  Trend Micro Email Security automatically blocks messages sent from addresses or domains added to the blocked list without submitting the messages to any scanning.

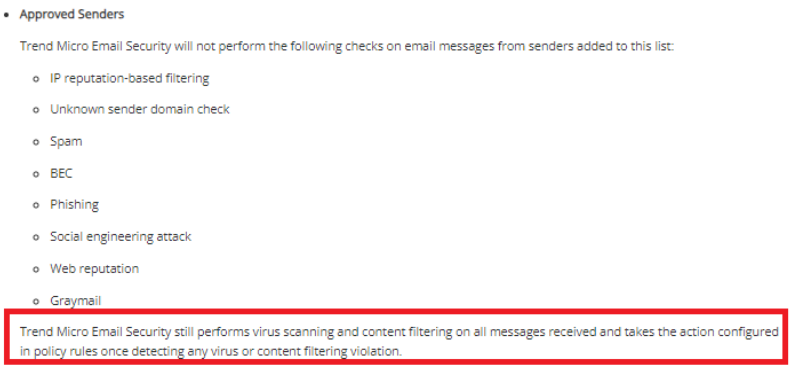
The **Approved Senders** and **Blocked Senders** tables display the following information:

- **Status**: Specifies whether the senders added to a recipient are enabled
- **Recipient**: The recipient for which you approved or blocked the specified sender. The options include the entire organization, a managed domain, or a specific recipient address in a managed domain.

33. On information and belief, the Accused Products also perform risk determinations for received messages that include determining whether the message comprises a hyperlink and, in certain accused implementations, rewriting or replacing hyperlinks with proxy or rewritten hyperlinks for further analysis and protection. For example, Trend Micro documentation for Time-of-Click Protection states that Trend Micro rewrites URLs in email messages for further analysis and analyzes those URLs when clicked, and Trend Micro documentation for Deep Discovery Email Inspector similarly states that it rewrites URLs in email messages for further analysis and displays blocking or warning redirect pages, such as determining whether the message comprises a hyperlink.[3]

[3] *E.g.*, https://docs.trendmicro.com/en-us/documentation/article/trend-micro-email-security-online-help-configuring-time-of-?.

34. On information and belief, the Accused Products automatically perform security actions when messages are determined to pose a risk, including messages associated with trusted or approved senders, trusted domains, or organizational relationships. Such actions include marking up messages with warnings, rewriting hyperlinks, quarantining messages, blocking messages, and/or including information about the message in administrator-accessible reports, such as quarantining and/or reporting the message:[4]


- **Approved Senders**

  Trend Micro Email Security will not perform the following checks on email messages from senders added to this list:

  - IP reputation-based filtering
  - Unknown sender domain check
  - Spam
  - BEC
  - Phishing
  - Social engineering attack
  - Web reputation
  - Graymail

  Trend Micro Email Security still performs virus scanning and content filtering on all messages received and takes the action configured in policy rules once detecting any virus or content filtering violation.

35. Given the above and other publicly available information about the Accused Products, the Accused Products satisfy all claim limitations of one or more claims of each of the Asserted Patents, including Claim 1 of the '195 Patent and Claim 1 of the '336 Patent, as set forth in the Counts below.

COUNT I

DEFENDANT'S INFRINGEMENT OF U.S. PATENT NO. 10,721,195

36. ZapFraud realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

37. The claims of the '195 Patent relate to specific computer-implemented systems and methods for detecting and defending against email fraud and misuse, including BEC scams.

[4] https://docs.trendmicro.com/en-us/documentation/article/trend-micro-email-security-online-help-configuring-approved

The claimed techniques include determining trust relationships, evaluating whether messages present email-security risks, and automatically performing security, warning, quarantine, reporting, and related actions.

38. Claim 1 of the ’195 Patent recites, among other things, a system for detection of business email compromise that automatically determines that a first party is trusted by a second party, receives a message addressed to the second party from a third party distinct from the first party, performs a risk determination based on display-name or domain-name similarity, and automatically performs security and report-generation actions when the message is determined to pose a risk.

39. The claims of the ’195 Patent are valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

40. Defendant’s infringing activities violate 35 U.S.C. § 271.

41. Defendant infringes at least Claim 1 of the ’195 Patent. *See e.g.*, ’195 Patent at 3: 17–39

42. For example, Claim 1 of the ’195 Patent recites:

> 1. A system for detection of business email compromise, comprising:
>
> a processor configured to:
>
> automatically determine that a first party is trusted by a second party, based on at least one of determining that the first party and second party belong to the same organization and that at least a threshold number of messages have been transmitted between the second party and the first party during a period of time that exceeds a threshold time;
>
> receive a message addressed to the second party from a third party, the third party distinct from the first party;
>
> perform a risk determination of the message to determine if the message poses a risk by determining that a display name of the first party and a display name of third party are the same or that a domain name of the first party and a domain name of the third party are similar, wherein similarity is determined based on having a string distance below a first threshold, or

being conceptually similar based on a list of conceptually similar character strings;

responsive to the first party being trusted by the second party, and the message is determined to pose a risk, automatically perform a security action and a report generation action without having received any user input from a user associated with the second party in response to the message, wherein the security action comprises marking the message up with a warning or quarantining the message, wherein the report generating action comprises including information about the message in a report accessible to an admin of the system; and

a memory coupled to the processor and configured to provide the processor with instructions.

43. The Accused Products satisfy all limitations of one or more claims of the '195 Patent, including Claim 1. Defendant has infringed and continues to directly infringe one or more claims of the '195 Patent by making, using, selling, offering for sale, distributing, importing, advertising, administering, supporting, and/or providing the Accused Products in the United States. To the extent any element is not literally present, each such element is present under the doctrine of equivalents. A comparison of Claim 1 of the '195 Patent to the Accused Products is attached as Exhibit 3 and incorporated by reference.

44. Defendant also knowingly and intentionally induces infringement of at least Claim 1 of the '195 Patent in violation of 35 U.S.C. § 271(b). Defendant has had knowledge of the '195 Patent and ZapFraud's infringement allegations no later than service of this Complaint. Despite that knowledge, Defendant continues to encourage, instruct, and assist customers, end users, and/or other third parties to use the Accused Products in a manner that infringes the '195 Patent. On information and belief, Defendant knows and intends that such customers, end users, and/or other third parties will commit infringing acts through their normal and customary use of the Accused Products.

45. To the extent discovery confirms that particular components or functionality of the Accused Products constitute a material part of the inventions claimed in the '195 Patent, are

especially made or adapted for infringing use, and are not staple articles or commodities of commerce suitable for substantial non-infringing use, Defendant has contributorily infringed and continues to contributorily infringe the '195 Patent under 35 U.S.C. § 271(c).

46. By making, using, offering for sale, selling, and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the '195 Patent under 35 U.S.C. § 271.

47. As a result of Defendant's infringement of the '195 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use of the invention by Defendant, together with interest and costs as fixed by the Court.

48. Defendant has had knowledge of the '195 Patent and ZapFraud's infringement allegations no later than service of this Complaint. On information and belief, despite that knowledge, Defendant has continued and will continue to infringe the '195 Patent. Defendant's post-notice infringement has been and continues to be willful.

49. Defendant's infringing activities have injured and will continue to injure ZapFraud unless and until this Court enters an injunction prohibiting further infringement of the '195 Patent, including further unauthorized making, use, sale, offer for sale, importation, distribution, provision, administration, support, and/or use of products and services that come within the scope of the '195 Patent's claims.

COUNT II

DEFENDANT'S INFRINGEMENT OF U.S. PATENT NO. 11,595,336

50. ZapFraud realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

51. The claims of the ’336 Patent relate to specific computer-implemented systems and methods for detecting and defending against email fraud and misuse, including BEC scams. The claimed techniques include determining whether a party is trusted or considered trusted, evaluating message risk based on hyperlinks, display-name similarity, and/or domain-name similarity, and automatically performing security, warning, quarantine, report-generation, proxy-link, and related actions.

52. The abstract of the ’336 Patent generally describes one exemplary implementation: “A system for detection of email risk automatically determines that a first party is considered by the system to be trusted by a second party, based on at least one of determining that the first party is on a whitelist and that the first party is in an address book associated with the second party. A message addressed to the second party from a third party is received. A risk determination of the message is performed by determining whether the message comprises a hyperlink and by determining whether a display name of the first party and a display name of third party are the same or that a domain name of the first party and a domain name of the third party are similar, wherein similarity is determined based on having a string distance below a first threshold or being conceptually similar based on a list of conceptually similar character strings. Responsive to determining that the message poses a risk, a security action is automatically performed comprising at least one of marking the message up with a warning, quarantining the message, performing a report generating action comprising including information about the message in a report accessible to an admin of the system, and replacing the hyperlink in the message with a proxy hyperlink.” ’336 Patent at abstract.

53. The claims of the ’336 Patent are valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

54. Defendant's infringing activities violate 35 U.S.C. § 271.

55. Defendant infringes at least Claim 1 of the '336 Patent.

56. For example, Claim 1 of the '336 Patent recites:

> 1. A system for detection of email risk, comprising:
>
> a processor configured to:
>
> automatically determine that a first party is considered by the system to be trusted by a second party, based on at least one of determining that the first party is on a whitelist and that the first party is in an address book associated with the second party;
>
> receive a message addressed to the second party from a third party, the third party distinct from the first party;
>
> perform a risk determination of the message by determining whether the message comprises a hyperlink and by determining whether a display name of the first party and a display name of third party are the same or that a domain name of the first party and a domain name of the third party are similar, wherein similarity is determined based on having a string distance below a first threshold or being conceptually similar based on a list of conceptually similar character strings;
>
> responsive to the first party being trusted by the second party, and that the message is determined to pose a risk, automatically perform a security action and a report generation action without having received any user input from a user associated with the second party in response to the message, wherein the security action comprises replacing the hyperlink in the message with a proxy hyperlink, wherein the report generating action comprises including information about the received message in a report accessible to an admin of the system; and
>
> a memory coupled to the processor and configured to provide the processor with instructions.

57. While the claims of the '336 Patent share many similarities with the claims of the '195 Patent, there are notable differences. For example, Claim 1 of the '336 Patent describes automatically determining whether the first party is trusted based on it being on the second party's whitelist and in its address book, which differs from Claim 1 of the '195 Patent. Claim 1 of the '336 Patent also considers an additional risk assessment factor by determining whether the message at issue comprises a hyperlink.

58. The Accused Products satisfy all limitations of one or more claims of the ’336 Patent, including Claim 1. Defendant has infringed and continues to directly infringe one or more claims of the ’336 Patent by making, using, selling, offering for sale, distributing, importing, advertising, administering, supporting, and/or providing the Accused Products in the United States. To the extent any element is not literally present, each such element is present under the doctrine of equivalents. A comparison of Claim 1 of the ’336 Patent to the Accused Products is attached as Exhibit 4 and incorporated by reference.

59. Defendant also knowingly and intentionally induces infringement of at least Claim 1 of the ’336 Patent in violation of 35 U.S.C. § 271(b). Defendant has had knowledge of the ’336 Patent and ZapFraud’s infringement allegations no later than service of this Complaint. Despite that knowledge, Defendant continues to encourage, instruct, and assist customers, end users, and/or other third parties to use the Accused Products in a manner that infringes the ’336 Patent. On information and belief, Defendant knows and intends that such customers, end users, and/or other third parties will commit infringing acts through their normal and customary use of the Accused Products.

60. To the extent discovery confirms that particular components or functionality of the Accused Products constitute a material part of the inventions claimed in the ’336 Patent, are especially made or adapted for infringing use, and are not staple articles or commodities of commerce suitable for substantial non-infringing use, Defendant has contributorily infringed and continues to contributorily infringe the ’336 Patent under 35 U.S.C. § 271(c).

61. By making, using, offering for sale, selling, and/or importing into the United States the Accused Products, Defendant has injured Plaintiff and is liable for infringement of the ’336 Patent under 35 U.S.C. § 271.

62. As a result of Defendant's infringement of the '336 Patent, Plaintiff is entitled to monetary damages in an amount adequate to compensate for Defendant's infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendant, together with interest and costs as fixed by the Court.

63. Defendant has had knowledge of the '336 Patent and ZapFraud's infringement allegations no later than service of this Complaint. On information and belief, despite that knowledge, Defendant has continued and will continue to infringe the '336 Patent. Defendant's post-notice infringement has been and continues to be willful.

64. Defendant's infringing activities have injured and will continue to injure ZapFraud unless and until this Court enters an injunction prohibiting further infringement of the '336 Patent, including further unauthorized making, use, sale, offer for sale, importation, distribution, provision, administration, support, and/or use of products and services that come within the scope of the '336 Patent's claims.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

(a) A judgment in favor of Plaintiff that Defendant has infringed the '195 Patent and the '336 Patent;

(b) A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant's infringement of the '195 Patent and the '336 Patent;

(c) A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant;

(d) An award of enhanced damages to Plaintiff as a result of Defendant's willful infringement;

(e) An injunction prohibiting further infringement of the ’195 Patent and the ’336 Patent and, specifically, enjoining further manufacture, use, sale, importation, and/or offers for sale that come within the scope of the patent claims; and

(f) Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, ZapFraud hereby demands a trial by jury on all issues so triable by right.

Dated: July 20, 2026

Respectfully submitted,

/s/ Robert M. Harkins

Robert M. Harkins
CA Bar No. 179525
Cherian Harkins Dunham LLP
555 12th Street, Suite 2140
Oakland, CA 94607
bobh@chdlaw.com
Telephone: (510) 944-0190

Thomas M. Dunham
DC Bar No. 448407
J. Michael Woods
DC Bar No. 975433
Stephanie R. Wood
TX Bar No. 24057928
Cherian Harkins Dunham LLP
2001 L St. NW, Suite 650
Washington, DC 20036
tomd@chdlaw.com
michaelw@chdlaw.com
stephaniew@chdlaw.com
Telephone: (202) 838-1560

ATTORNEYS FOR PLAINTIFF ZAPFRAUD, INC.