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

ZAPFRAUD, INC., **PLAINTIFF,** **v.** **GOOGLE LLC and** **THE WURSTA CORPORATION,** **Defendants.**	**Case No. _____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff ZapFraud, Inc. ("ZapFraud") brings this action against Defendants Google LLC ("Google") and The Wursta Corporation ("Wursta") (collectively, "Defendants") 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 arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*., based on Defendants' infringement of the Asserted Patents.

2. ZapFraud owns the entire right, title, and interest in and to each of the Asserted Patents, including the right to sue for and recover damages for past, present, and future infringement, including rights to sue and recover lost profits, royalties, and damages.

3. Without authorization from ZapFraud, Google makes, uses, sells, offers for sale, and/or imports into the United States products and services that infringe the Asserted Patents,

including Google Workspace, Gmail for business, and email-security functionality within those services, including anti-phishing, anti-spoofing, suspicious-link, business-email-compromise, warning, quarantine, reporting, and administrative functionality (the "Google Accused Products"). Without authorization from ZapFraud, Wursta sells, offers for sale, implements, configures, administers, supports, trains customers on, and/or provides services relating to Google Workspace and associated Gmail email-security functionality for customers, including Google Workspace migration, onboarding, optimization, premium support, managed services, virtual administration, security assessments, administrator training, and related support services (the "Wursta Accused Services," and together with the Google Accused Products, the "Accused Instrumentalities").

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 and 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 over 200 publications, and the inventor or co-inventor of over 375 patents.

7. On information and belief, Defendant Google LLC is a Delaware limited liability company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

8. On information and belief, Google maintains places of business in Texas, including a physical address in this District at 500 West 2nd Street, Austin, Texas, 78701.

9. On information and belief, Defendant The Wursta Corporation is a corporation organized under the laws of Pennsylvania and headquartered at 1021 E 7th St, Austin, Texas 78702.

10. On information and belief, Defendants Google and Wursta conduct business in Texas, including this District.

11. On information and belief, each Defendant maintains a regular and established place of business in this District. Google maintains a regular and established place of business in this District, including at 500 West 2nd Street, Austin, Texas 78701. Wursta maintains a regular and established place of business in this District, including its headquarters at 1021 East 7th Street, Austin, Texas 78702. Google may be served with process through its Texas registered agent, Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, at 211 East 7th Street, Suite 620, Austin Texas 78701-3218. Wursta can be served with process through its Texas registered agent, Northwest Registered Agent, LLC, at 211 East 7th Street, Suite 620, Austin Texas 78701.

12. On information and belief, Google designs, develops, makes, uses, sells, offers to sell, distributes, advertises, and/or imports the Google Accused Products in the United States, including throughout the State of Texas and this District. On information and belief, Wursta sells, offers to sell, implements, configures, administers, trains customers on, supports, and/or provides services relating to Google Workspace and associated Gmail email-security functionality in the United States, including throughout the State of Texas and this District.

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

JURISDICTION AND VENUE

14. This Court has personal jurisdiction over Defendants under the Texas Long Arm Statute. Defendants have purposefully directed infringing activities toward Texas and this District, including by making, using, selling, offering for sale, distributing, advertising, implementing, supporting, and/or providing the Accused Products and Wursta Accused Services in Texas and this District. ZapFraud's claims arise out of and relate to those activities. Exercising jurisdiction over Defendants in this District thus comports with Due Process.

15. Defendants have purposefully availed themselves of the laws and protections of the United States and the State of Texas. On information and belief, Google directly and/or through authorized partners, resellers, service providers, and intermediaries offers, sells, distributes, administers, and supports Google Workspace, Gmail for business, and related email-security functionality to customers in Texas and this District. On information and belief, Wursta, a Google Workspace and Google Cloud service provider headquartered in this District, offers, sells, implements, configures, administers, trains customers on, and supports Google Workspace and related services for customers in Texas and this District. On information and belief, Defendants derive substantial revenue from the Accused Products and Wursta Accused Services in Texas and this District, and ZapFraud's infringement claims arise from and relate to those Texas-directed activities.

16. ZapFraud's claims for patent infringement arise directly from and relate to Defendants' activities in this District, including Google's making, using, selling, offering for sale, distributing, administering, and supporting the Google Accused Products in this District,

and Wursta's selling, offering for sale, implementing, configuring, administering, training customers on, supporting, and providing the Wursta Accused Services in this District.

17. Venue is proper in this District under 28 U.S.C. § 1400(b) because, on information and belief, Defendants have committed acts of infringement in this District and maintain regular and established places of business in this District.

18. On information and belief, Defendants maintain regular and established places of business in this District. Google maintains an Austin office at 500 West 2nd Street, Austin, Texas 78701. Wursta maintains its headquarters at 1021 East 7th Street, Austin, Texas 78702.

19. On information and belief, relevant sources of proof and witnesses are located in this District, including Wursta personnel and documents concerning Wursta's offer, sale, implementation, configuration, administration, training, and support of Google Workspace and related services. On information and belief, Google also maintains employees and business operations in this District.

THE ASSERTED PATENTS

20. 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.

21. 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.

22. 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 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.

23. 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.

24. 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.

25. 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, 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.

26. 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

27. Defendants have, without ZapFraud's authority, engaged in acts of infringement involving the Accused Products. Google has made, used, sold, offered to sell, distributed, imported, advertised, and/or provided the Google Accused Products in the United States, including Google Workspace, Gmail for business, and related anti-phishing, anti-spoofing, suspicious-link, warning, quarantine, reporting, and administrator functionality. Wursta has sold, offered to sell, implemented, configured, administered, trained customers on, supported, and provided services relating to Google Workspace and related email-security functionality, and has instructed and assisted customers in using those services. ZapFraud's allegations against Wursta are based on Wursta's sale, implementation, configuration, administration, training, support, and customer enablement of Google Workspace and related Gmail email-security functionality, including any Wursta use of that functionality in providing such services. By doing so, and as alleged in more detail below, Defendants directly infringe, and at least after service of this Complaint knowingly induce and/or contribute to infringement of, one or more claims of the Asserted Patents, literally and/or under the doctrine of equivalents.

28. On information and belief, Google directly and indirectly, including through affiliates, subsidiaries, agents, partners, resellers, service providers, customers, and/or other intermediaries, makes, uses, sells, offers for sale, distributes, imports, advertises, administers, and supports the Google Accused Products in the United States, including in this District. On information and belief, Wursta directly and indirectly sells, offers for sale, implements, configures, administers, trains customers on, supports, and provides the Wursta Accused Services in the United States, including in this District, including by enabling customer use of Google Workspace and related Gmail email-security functionality.

29. Defendants have had knowledge of the Asserted Patents and of ZapFraud's allegations that the Accused Products infringe the Asserted Patents no later than service of this Complaint. On information and belief, Defendants have continued and will continue their 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 Google Accused Products and Wursta Accused Services. ZapFraud reserves all rights, including the right to modify this description based on information obtained during discovery.

31. On information and belief, the Google Accused Products include systems for detecting email risk, including BEC scams. For example, Google Workspace includes advanced security settings and email-security functionality for detecting and responding to suspicious attachments, suspicious links and external images, spoofing, authentication issues, employee-

name spoofing, domain spoofing, unauthenticated emails, and potential BEC messages. On information and belief, Google Workspace also allows administrators to configure actions for detected email risks, including warning banners, spam handling, quarantine, reporting, and related administrative actions. On information and belief, Wursta sells, implements, configures, administers, trains customers on, supports, and provides services relating to Google Workspace and its email-security functionality through the Wursta Accused Services.[1]

[1] https://knowledge.workspace.google.com/admin/gmail/advanced/advanced-phishing-and-malware-protection

Advanced security settings

- **Attachments**—Protection against suspicious attachments and scripts from untrusted senders. Includes protection against attachments types that are uncommon for your domain—these can be used to spread malware.
- **Links and external images**—Identify links behind short URLs, scan linked images for malicious content, and display a warning when you click links to untrusted domains.
- **Spoofing and authentication**—Protection against spoofing a domain name, employee names, email pretending to be from your domain, and unauthenticated email from any domain. Unauthenticated emails display a question mark next to the sender's name. Spoofing protection can be turned on for private groups, or for all groups.

With advanced settings, you can:

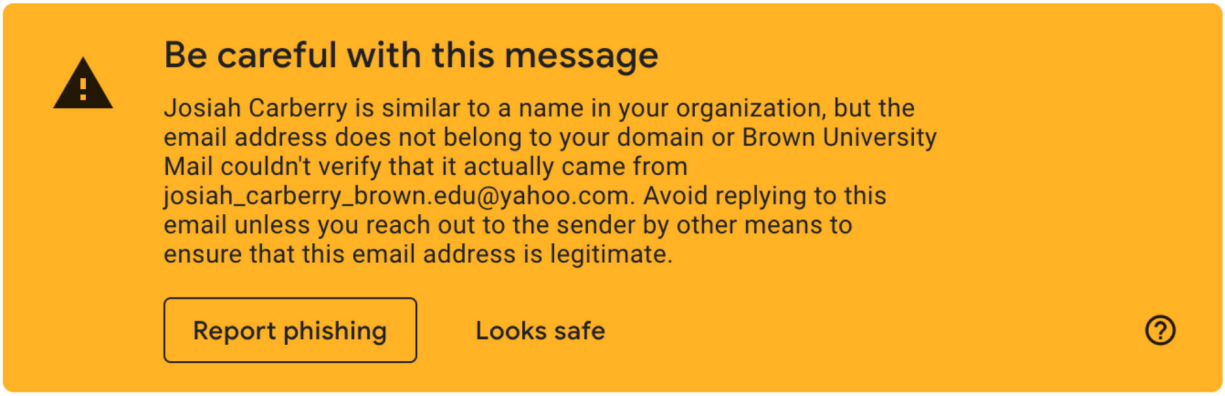
- Automatically turn on and apply future recommended settings. This ensures maximum protection for email and attachments for your domain.
- Provide the strongest level of protection for a domain or organizational unit by turning on all security options.
- Customize security settings by checking only the options you want to turn on. Unchecking all options turns off all advanced security settings for the domain or organizational unit.
- Specify an action for each security option you turn on. If you don't select an action, the default action is applied to the security option.

Keep in mind:

- **Other spam settings**—Generally, these advanced security features work independently of other spam settings you might have previously turned on. For example, even if you've listed a domain as a safe sender in spam settings, the enhanced security features are still applied.
- **Warning banners**—Certain Spam setting options prevent warning banners for possibly malicious messages. When you select either of these Spam setting options, Gmail never displays warning banners: **Bypass spam filters and hide warnings for messages from senders or domains in selected lists** and **Bypass spam filters and hide warnings for all messages from internal and external senders**. Warning banners (yellow box) appear only in Gmail web. Third-party apps do not display a warning banner.
- **Quarantine action**—When you select **Quarantine** for any of the advanced security settings, the quarantine you select applies *only* to incoming messages. This is true even when the quarantine you select specifies actions to take on outgoing messages. Allowlist settings don't override the **Quarantine** option.

32. On information and belief, the Google Accused Products provide electronic-security functionality that automatically determines whether a first party is trusted or considered trusted by a second party, including, depending on the applicable asserted claim, by determining whether parties belong to the same organization, whether a threshold number of messages have

been transmitted over a threshold time period, whether the first party is on a whitelist, and/or whether the first party is in an address book or directory associated with the second party. For example, Google Workspace detects employee-name spoofing and messages that appear to come from a trusted or known sender but originate from a different address.[2]



33. On information and belief, the Google Accused Products perform risk determinations for received messages, including by determining whether a message comprises a hyperlink, whether a display name matches or is similar to a trusted party's display name, whether a domain name is similar to a trusted party's domain name, and/or whether the message presents spoofing, authentication, suspicious-link, or BEC-related risk.[3]

34. On information and belief, the Google Accused Products automatically perform security, warning, quarantine, reporting, link-protection, proxy-link, and/or administrative actions in response to messages determined to pose an email-security risk. On information and belief, Wursta sells, implements, configures, administers, trains customers on, supports, and provides services relating to such Google Workspace and Gmail email-security functionality.

[2] https://ithelp.brown.edu/kb/articles/gmail-anti-spoofing-warning-banner; *see also* https://knowledge.workspace.google.com/admin/gmail/advanced/advanced-phishing-and-malware-protection.

[3] *See*, *e.g.*, https://support.google.com/mail/answer/10173182?hl=en.

35. Given the above and other publicly available information about the Google Accused Products, the Google Accused Products satisfy all limitations of one or more claims of each Asserted Patent, including Claim 1 of the '195 Patent and Claim 1 of the '336 Patent. Wursta's sale, implementation, configuration, administration, training, support, customer enablement, and provision of services relating to the Google Accused Products constitutes infringement and/or supports induced and contributory infringement as set forth in the Counts below.

COUNT I

DEFENDANTS' 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. 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. Defendants' infringing activities violate 35 U.S.C. § 271.

41. Defendants infringe at least Claim 1 of the '195 Patent.

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 Google Accused Products satisfy all limitations of one or more claims of the '195 Patent, including Claim 1. Google 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 Google Accused Products in the United States. Wursta has infringed and continues to directly infringe one or more claims of the '195 Patent by selling, offering for sale, implementing, configuring, administering,

training customers on, supporting, and providing services relating to Google Workspace and related Gmail email-security functionality, including by enabling customer use of such functionality. 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 (Google) and Exhibit 4 (Wursta) and incorporated by reference.

44. Defendants also knowingly and intentionally induce infringement of at least Claim 1 of the '195 Patent in violation of 35 U.S.C. § 271(b). Defendants have had knowledge of the '195 Patent and ZapFraud's infringement allegations no later than service of this Complaint. Despite that knowledge, Google continues to encourage, instruct, and assist customers and end users to use the Google Accused Products in a manner that infringes the '195 Patent. Despite that knowledge, Wursta continues to encourage, instruct, train, configure, administer, support, and assist customers and end users in using Google Workspace and related Gmail email-security functionality in a manner that infringes the '195 Patent. On information and belief, Defendants know and intend that such customers and end users will commit infringing acts through their normal and customary use of the Google Accused Products and Wursta Accused Services.

45. To the extent discovery confirms that particular components or functionality of the Google Accused Products, including functionality sold, implemented, configured, administered, supported, or enabled through the Wursta Accused Services, 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, Defendants have contributorily infringed and continue to contributorily infringe the '195 Patent under 35 U.S.C. § 271(c).

46. By making, using, offering for sale, selling, importing, distributing, administering, supporting, implementing, configuring, training on, and/or providing the Google Accused Products and Wursta Accused Services, Defendants have injured Plaintiff and are liable for infringement of the ’195 Patent under 35 U.S.C. § 271.

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

48. Defendants have 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, Defendants have continued and will continue to infringe the ’195 Patent. Defendants’ post-notice infringement has been and continues to be willful.

49. Defendants’ 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, implementation, configuration, administration, training, support, and/or use of products and services that come within the scope of the ’195 Patent’s claims.

COUNT II

DEFENDANTS’ 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. Defendants’ infringing activities violate 35 U.S.C. § 271.

55. Defendants infringe 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 requires automatically determining whether the first party is trusted based on it being on the second party’s whitelist or in its address book, which differs from Claim 1 of the ’195 Patent. Claim 1 of the ’336 Patent also adds a risk-assessment factor based on whether the message comprises a hyperlink.

58. The Google Accused Products satisfy all limitations of one or more claims of the ’336 Patent, including Claim 1. Google 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 Google Accused Products in the United States. Wursta has infringed and continues to directly infringe one or more claims of the ’336 Patent by selling, offering for sale, implementing, configuring, administering, training customers on, supporting, and providing services relating to Google Workspace and related Gmail email-security functionality, including by enabling customer use of such functionality. 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 5 (Google) and Exhibit 6 (Wursta) and incorporated by reference.

59. Defendants also knowingly and intentionally induce infringement of at least Claim 1 of the ’336 Patent in violation of 35 U.S.C. § 271(b). Defendants have had knowledge of the ’336 Patent and ZapFraud’s infringement allegations no later than service of this Complaint. Despite that knowledge, Google continues to encourage, instruct, and assist customers and end users to use the Google Accused Products in a manner that infringes the ’336 Patent. Despite that knowledge, Wursta continues to encourage, instruct, train, configure, administer, support, and assist customers and end users in using Google Workspace and related Gmail email-security functionality in a manner that infringes the ’336 Patent. On information and belief, Defendants know and intend that such customers and end users will commit infringing acts through their normal and customary use of the Google Accused Products and Wursta Accused Services.

60. To the extent discovery confirms that particular components or functionality of the Google Accused Products, including functionality sold, implemented, configured, administered, supported, or enabled through the Wursta Accused Services, 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, Defendants have contributorily infringed and continue to contributorily infringe the ’336 Patent under 35 U.S.C. § 271(c).

61. By making, using, offering for sale, selling, importing, distributing, administering, supporting, implementing, configuring, training on, and/or providing the Google Accused Products and Wursta Accused Services, Defendants have injured Plaintiff and are liable for infringement of the ’336 Patent under 35 U.S.C. § 271.

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

63. Defendants have 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, Defendants have continued and will continue to infringe the ’336 Patent. Defendants’ post-notice infringement has been and continues to be willful.

64. Defendants’ 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, implementation, configuration, administration, training, 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 Defendants have infringed the ’195 Patent and the ’336 Patent;

(b) A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendants' 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 Defendants;

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

(e) An injunction prohibiting further infringement of the '195 Patent and the '336 Patent, including unauthorized making, use, sale, offer for sale, importation, distribution, provision, implementation, configuration, administration, training, support, and/or use of products and services 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.