IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ZapFraud, Inc. Plaintiff, v. FireEye, Inc. Defendant.	Civil Action No. 19-cv-1688-CFC **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT

Plaintiff ZapFraud, Inc. ("ZapFraud"), for its Complaint against defendant FireEye, Inc. ("Defendant" or "FireEye"), hereby alleges as follows:

Introduction

1. ZapFraud is a technology company founded by leading email security researcher Dr. Bjorn Markus Jakobsson. ZapFraud innovates in the area of email security and provides email security solutions. Among other things, ZapFraud's patented technology automatically and reliably identifies threats to email including Business Email Compromise scams—a growing threat that has caused a total of over $12.5 billion of global reported losses as of 2018—and protects businesses and their employees against email-based deception and fraud attacks.

2. FireEye has used, and continues to use ZapFraud's patented technology.

Nature Of The Action

3. This action arises under 35 U.S.C. § 271 for FireEye's infringement of ZapFraud's United States Patent Nos. 10,277,628 ("the '628 patent") and 10,609,073 ("the '073 patent") (collectively "patents-in-suit").

The Parties

4. Plaintiff ZapFraud is a Delaware corporation with its principal place of business at 118 Ramona Rd, Portola Valley, CA 94028. ZapFraud is operated and controlled by Dr. Jakobsson.

5. Defendant FireEye is a Delaware corporation with its principal place of business at 601 McCarthy Blvd., Milpitas, CA 95035. FireEye may be served with process through its registered agent, Cogency Global Inc. at 850 New Burton Road Suite 201, Dover, DE 19904.

6. FireEye provides on premise as well as cloud-based email security solutions. Those solutions use and benefit from Dr. Jakobsson's patented technology, including the patents-in-suit.

Jurisdiction And Venue

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

8. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b) and (c), and 1400(b), because, among other things: FireEye is incorporated under the laws of the State of Delaware; FireEye has committed, aided, abetted, contributed to, and/or participated in the commission of acts giving rise to this action within the State of Delaware and this judicial district and has established minimum contacts within the forum such that the exercise of jurisdiction over FireEye would not offend traditional notions of fair play and substantial justice; FireEye has placed products and services that practice the claims of the patents-in-suit into the stream of commerce with the reasonable expectation or knowledge that actual or potential users of such products or services were located within this judicial district; and FireEye has sold, advertised, solicited customers, and marketed and distributed its products and services that practice the claims of the patents-in-suit in this judicial district.

Background Facts

9. Dr. Jakobsson founded ZapFraud in 2014.

10. ZapFraud pioneered the detection of Business Email Compromise scams through automated analysis of deceptive content and structure, and takes actions to, for example, quarantine, discard, tag, or deliver the incoming emails.

11. Dr. Jakobsson is and has been a frequent speaker on email fraud prevention, including on ZapFraud's fraud detection technology at industry events and conferences, such as RSA Conference 2016, Black Hat USA 2015, and RSA Conference 2014.

12. Defendant FireEye attends such industry events and conferences as a sponsor and/or an exhibitor. Such conferences permit attendees to learn about important developments in information and email security through first-hand interactions with peers, luminaries, and emerging and established companies. For example, FireEye attended RSA conference 2016, Black Hat USA 2015, and RSA Conference 2014, industry conferences where Dr. Jakobsson presented.

COUNT I

Infringement Of The '628 Patent

13. ZapFraud incorporates by reference the preceding paragraphs as if fully set forth herein.

14. The '628 patent, entitled "Detecting Phishing Attempts," was duly and legally issued by the United States Patent and Trademark Office on April 30, 2019 and corrected on October 8, 2019. A copy of the '628 patent is attached hereto as Exhibit A. Dr. Jakobsson is the sole inventor of the '628 patent.

15. ZapFraud is the exclusive owner of all rights, title, and interest of the ’628 patent, and has the right to bring this suit for injunctive relief and to recover damages for any current or past infringement of the ’628 patent.

16. The ’628 patent generally relates to a system, method, and computer program for detecting fraud or phishing attempts in email communications.

17. The ’628 patent is valid and enforceable.

18. At the time of the invention of the ’628 patent, email services used various technologies such as whitelisting, blacklisting, Domain-based Message Authentication, Reporting & Conformance (“DMARC”), and Domain Keys Identified Mail (“DKIM”) to protect email recipients from potential spam, fraud, or phishing attempts.

19. However, existing technologies could be readily defeated by unscrupulous individuals who craft spam, fraud, scam, or phishing emails. For example, the unscrupulous individual may use terms that a human would recognize, but might not appear on a blacklist. As another example, existing technologies were not capable of detecting a type of phishing-attempt emails that incorporate human-readable content indications of association of a message with an authoritative entity, and thus appear to be legitimate/trustworthy to a recipient. The degree of possible customization of electronic communications makes it particularly difficult for existing email filters to provide sufficient protection.

20. The invention of the ’628 patent solves the problems with existing technologies by, for example, combining an assessment of the likely end-user interpretation of the message with an assessment of whether the apparent sender matches the actual sender, and taking action in response, such as filtering or reporting the message.

21. In violation of 35 U.S.C. § 271, FireEye has infringed and/or induced others to infringe one or more claims of the ’628 patent by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States, products, solutions, systems, and services encompassed by those claims, including email security products and services that scan the display name of emails to identify email security threats, including, but not limited to, FireEye Email Security solutions.

22. FireEye provides email security products and services that protect customers against email-based targeted social engineering attacks known as Business Email Compromise.

23. FireEye’s email security products and services such as FireEye Email Security solutions analyze attributes of incoming emails including, for example, email headers, reply-to addresses, and display names to detect and block impersonation emails.

24. For example, FireEye infringes at least claim 1 of the ’628 patent through its classification system (such as FireEye Email Security solutions) for detecting attempted deception in an electronic communication (such as an incoming email), comprising:

a. a client device (such as a FireEye Email Security customer portal) used to access the electronic communication addressed to a user of the client device;

b. at least one of a profile and content database (such as such as where FireEye stores information used for impersonation analysis); and

c. at least one server (such as a FireEye Email Security server) in communication with the client device and the at least one of the profile and content database, the at least one server comprising:

i. an interface configured to receive the electronic communication; and

ii. a set of one or more processors configured to:

1. parse a display name associated with the electronic communication;
2. determine, by at least one classifier component (such as a component for impersonation detection), that the electronic communication appears to have been transmitted on behalf of an authoritative entity (such as an employee of a FireEye customer) by:
    a. computing a similarity distance between the display name and at least a name of the authoritative entity (such as the name of the customer employee), wherein the name of the authoritative entity is retrieved from the at least one of the profile and the content database, wherein the similarity distance is computed by comparison of items by at least one of:
        i. basing the comparison on at least one of a match between the display name of the electronic communication (such as the display name of the incoming email's sender) and the display name of the authoritative entity, and
        ii. a match between headers associated with the electronic communication (such as the header of the incoming email) and headers associated with the authoritative entity (such as the email header of the customer employee),

iii. wherein the matches are determined by at least one of: determining that the compared items are the same, determining that the compared items have a Hamming distance below a threshold value, determining that the compared items have an edit distance below a threshold value, determining that a support vector machine indicates a similarity based on previously trained examples, determining a similarity score based on how many characters were replaced by characters of sufficient similarity and performing at least one normalization followed by a comparison (such as by generating a MD5 hash result of at least a portion of the incoming email's header information and comparing that with information that has been set by the FireEye customer, and/or using a metaphone or string similarity algorithm);

3. determine, by the at least one classifier component, that the electronic communication was not transmitted with authorization from the authoritative entity (such as by analyzing, for example, the incoming email's header email address, reply-to email address, and/or content);

4. based at least in part on determining that the electronic communication appears to have been transmitted on behalf of the

authoritative entity and determining that the electronic communication was not transmitted with authorization from the authoritative entity, perform a security determination including classifying the electronic communication, wherein the classifying includes two or more security classifications including good and bad (such as by determining that an incoming email is an impersonation attack based on for example, friendly display name matching, looks-like and sounds-like domain analysis, and/or reply-to address and message header analysis); and

5. based at least in part on the security determination resulting in a bad classification, perform an action comprising at least one of erasing the electronic communication, marking up the electronic communication at least in part by adding a warning or an explanation, flagging the electronic communication, forwarding the electronic communication to a third party, placing the electronic communications in the spam folder, and forwarding the electronic communication to a repository (such as by blocking the email or quarantining the email); and

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

25. FireEye infringes at least claim 1 of the ’628 patent under 35 U.S.C. § 271(a) by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States such a classification system. For example, FireEye makes the system by providing

all the components of the system and combining the components into an infringing system. As another example, FireEye uses the system by placing the system into service, exercising control of the system, and obtaining benefits from using the system.

26. Third parties, including FireEye's customers and partners, have infringed, and continue to infringe, one or more claims of the '628 patent under 35 U.S.C. § 271(a), either literally and/or under the doctrine of equivalents, by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States, FireEye email security products and services that scan the display name of emails to identify email security threats, including, but not limited to, FireEye Email Security solutions.

27. FireEye has had knowledge of and notice of the '628 patent and its infringement since at least the filing of this action.

28. FireEye has induced infringement, and continues to induce infringement, of one or more claims of the '628 patent under 35 U.S.C. § 271(b) since at least the filing of this action. FireEye actively, knowingly, and intentionally induced, and continues to actively, knowingly, and intentionally induce, infringement of the '628 patent by selling or otherwise supplying FireEye email security products and services that scan the display name of emails to identify email security threats, including, but not limited to, FireEye Email Security solutions, with the knowledge and intent that third parties will use, sell, and/or offer for sale in the United States, and/or import into the United States these products and services to infringe the '628 patent; and with the knowledge and intent to encourage and facilitate the infringement through the dissemination of these products and services and/or the creation and dissemination of promotional and marketing materials, supporting materials, instructions, product manuals, and/or technical information related to these products and services.

29. FireEye has contributed to the infringement by third parties, including FireEye's customers, and continues to contribute to infringement by third parties, of one or more claims of the '628 patent under 35 U.S.C. § 271(c) since at least the filing of this action, by selling and/or offering for sale in the United States, and/or importing into the United States, FireEye email security products and services that scan the display name of emails to identify email security threats, including, but not limited to, FireEye Email Security solutions, knowing that these products and services constitute a material part of the inventions of the '628 patent, knowing that these products and services are especially made or adapted to infringe the '628 patent, and knowing that these products and services are not staple articles of commerce suitable for substantial noninfringing use.

30. ZapFraud has been and continues to be damaged by FireEye's infringement of the '628 patent, and will suffer irreparable injury unless the infringement is enjoined by this Court.

31. FireEye's infringement of the '628 patent has been, and continues to be, willful since at least the filing of this action.

32. FireEye's conduct in infringing the '628 patent renders this case exceptional within the meaning of 35 U.S.C. § 285.

COUNT II

Infringement Of The '073 Patent

33. ZapFraud incorporates by reference the preceding paragraphs as if fully set forth herein.

34. The '073 patent, entitled "Detecting Phishing Attempts," was duly and legally issued by the United States Patent and Trademark Office on March 31, 2020. A copy of the '073 patent is attached hereto as Exhibit B. Dr. Jakobsson is the sole inventor of the '073 patent.

35. ZapFraud is the exclusive owner of all rights, title, and interest of the ’073 patent, and has the right to bring this suit for injunctive relief and to recover damages for any current or past infringement of the ’073 patent.

36. The ’073 patent generally relates to a system, method, and computer program for detecting fraud or phishing attempts in email communications.

37. The ’073 patent is valid and enforceable.

38. At the time of the invention of the ’073 patent, email services used various technologies such as whitelisting, blacklisting, Domain-based Message Authentication, Reporting & Conformance (“DMARC”), and Domain Keys Identified Mail (“DKIM”) to protect email recipients from potential spam, fraud, or phishing attempts.

39. However, existing technologies could be readily defeated by unscrupulous individuals who craft spam, fraud, scam, or phishing emails. For example, the unscrupulous individual may use terms that a human would recognize, but might not appear on a blacklist. As another example, existing technologies were not capable of detecting a type of phishing-attempt emails that incorporate human-readable content indications of association of a message with an authoritative entity, and thus appear to be legitimate/trustworthy to a recipient. The degree of possible customization of electronic communications makes it particularly difficult for existing email filters to provide sufficient protection.

40. The invention of the ’073 patent solves the problems with existing technologies by, for example, combining an assessment of the likely end-user interpretation of the message with an assessment of whether the apparent sender matches the actual sender, and taking action in response, such as filtering or reporting the message.

41. In violation of 35 U.S.C. § 271, FireEye has infringed and/or induced others to infringe one or more claims of the ’073 patent by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States, products, solutions, systems, and services encompassed by those claims, including, but not limited to, FireEye Email Security solutions.

42. For example, FireEye infringes at least claim 1 of the ’073 patent through its classification system (such as FireEye Email Security solutions) for detecting attempted deception in an electronic communication (such as an incoming email), comprising:

a. a client device (such as a FireEye Email Security customer portal) used to access the electronic communication addressed to a user of the client device;

b. at least one of a profile and content database (such as where FireEye stores information used for impersonation analysis); and

c. at least one server (such as a FireEye Email Security server) in communication with the client device and the at least one of the profile and content database, the at least one server comprising:

i. an interface configured to receive the electronic communication; and

ii. a set of one or more processors configured to:

1. determine, by at least one classifier component (such as a component for impersonation detection), that the electronic communication appears to have been transmitted on behalf of an authoritative entity (such as an employee of a FireEye customer) by:

a. computing a similarity distance between a first item from the electronic communication and a second item associated with

the authoritative entity, wherein the second item associated with the authoritative entity is retrieved from the at least one of the profile and content database, wherein the similarity distance is computed by performing a match between at least one of:

i. the first item comprising a display name of the electronic communication (such as the display name of the incoming email's sender) and the second item comprising a display name of the authoritative entity,

ii. the first item comprising an email address of a sender of the electronic communication and the second item comprising an email address of the authoritative entity,

iii. the first item comprising at least a part of a text comprising the electronic communication and the second item comprising at least a part of a text associated with the authoritative entity; and

iv. the first item comprising a header associated with the electronic communication (such as the header of the incoming email) and the second item comprising a header associated with the authoritative entity (such as the email header of the customer employee),

v. wherein the match is determined by at least one of: determining that first item and the second item are the same, determining that the first item and the second item have a Hamming distance below a first threshold value, determining that the first item and the second item have an edit distance below a second threshold value, determining that a support vector machine indicates a similarity between the first item and the second item based on previously trained examples, determining a similarity score based on how many characters in the second item were replaced by characters in the first item and performing at least one normalization prior to performing the match (such as by generating a MD5 hash result of at least a portion of the incoming email's header information and comparing that with information that has been set by the FireEye customer, and/or using a metaphone or string similarity algorithm);

2. determine, by the at least one classifier component, that the electronic communication was not transmitted with an authorization from the authoritative entity (such as by analyzing, for example, the

incoming email's header email address, reply-to email address, and/or content);

3. based at least in part on determining that the electronic communication appears to have been transmitted on behalf of the authoritative entity and determining that the electronic communication was not transmitted with the authorization from the authoritative entity, perform a security action comprising at least one of: erasing the electronic communication, marking up the electronic communication at least in part by adding a warning or an explanation, flagging the electronic communication, forwarding the electronic communication to a third party, placing the electronic communications in a spam folder, and forwarding the electronic communication to a repository (such as by blocking the email or quarantining the email); and

iii. a memory coupled to the set of one or more processors and configured to provide the set of one or more processors with instructions.

43. FireEye infringes at least claim 1 of the '073 patent under 35 U.S.C. § 271(a) by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States such a classification system. For example, FireEye makes the system by providing all the components of the system and combining the components into an infringing system. As another example, FireEye uses the system by placing the system into service, exercising control of the system, and obtaining benefits from using the system.

44. Third parties, including FireEye's customers and partners, have infringed, and continue to infringe, one or more claims of the '073 patent under 35 U.S.C. § 271(a), either literally and/or under the doctrine of equivalents, by making, using, selling, and/or offering for sale in the United States, and/or importing into the United States, products, solutions, systems, and services encompassed by those claims, including, but not limited to, FireEye Email Security solutions.

45. FireEye has had knowledge of and notice of the '073 patent and its infringement since at least the filing of this Complaint.

46. FireEye has induced infringement, and continues to induce infringement, of one or more claims of the '073 patent under 35 U.S.C. § 271(b) since at least the filing of this Complaint. FireEye actively, knowingly, and intentionally induced, and continues to actively, knowingly, and intentionally induce, infringement of the '073 patent by selling or otherwise supplying products, solutions, systems, and services encompassed by those claims, including, but not limited to, FireEye Email Security solutions, with the knowledge and intent that third parties will use, sell, and/or offer for sale in the United States, and/or import into the United States these products and services to infringe the '073 patent; and with the knowledge and intent to encourage and facilitate the infringement through the dissemination of these products and services and/or the creation and dissemination of promotional and marketing materials, supporting materials, instructions, product manuals, and/or technical information related to these products and services.

47. FireEye has contributed to the infringement by third parties, including FireEye's customers, and continues to contribute to infringement by third parties, of one or more claims of the '073 patent under 35 U.S.C. § 271(c) since at least the filing of this Complaint, by selling and/or offering for sale in the United States, and/or importing into the United States, products, solutions, systems, and services encompassed by those claims, including, but not limited to,

FireEye Email Security solutions, knowing that these products and services constitute a material part of the inventions of the ’073 patent, knowing that these products and services are especially made or adapted to infringe the ’073 patent, and knowing that these products and services are not staple articles of commerce suitable for substantial noninfringing use.

48. ZapFraud has been and continues to be damaged by FireEye’s infringement of the ’073 patent, and will suffer irreparable injury unless the infringement is enjoined by this Court.

49. FireEye’s infringement of the ’073 patent has been and continues to be willful since at least the filing of this Complaint.

50. FireEye’s conduct in infringing the ’073 patent renders this case exceptional within the meaning of 35 U.S.C. § 285.

Prayer For Relief

WHEREFORE, ZapFraud prays for judgment as follows:

A. That FireEye has infringed the patents-in-suit;

B. That FireEye’s infringement of the patents-in-suit has been willful;

C. That FireEye, its officers, agents, and employees, and those persons in active concert or participation with any of them, and their successors and assigns, be permanently enjoined from infringement, inducing infringement, and contributory infringement of the patents-in-suit, including but not limited to the making, using, selling, and/or offering for sale in the United States, and/or importing into the United States, any devices, products, software, or methods that infringe the patents-in-suit before their respective expiration dates;

D. That ZapFraud be awarded all damages adequate to compensate it for FireEye’s infringement, such damages to be determined by a jury and, if necessary to adequately compensate

ZapFraud for the infringement, an accounting, and that such damages be trebled and awarded to ZapFraud with pre-judgment and post-judgment interest;

E. That this case be declared an exceptional case within the meaning of 35 U.S.C. § 285 and that ZapFraud be awarded the attorney fees, costs, and expenses incurred in connection with this action; and

F. That ZapFraud be awarded such other and further relief as this Court deems just and proper.

Demand For Jury Trial

Plaintiff ZapFraud hereby demands a trial by jury on all issues so triable.

Dated: April 24, 2020

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan
Brian E. Farnan (No. 4089)
Michael J. Farnan (Bar No. 5165)
919 North Market St., 12th Floor
Wilmington, DE 19801
Telephone: 302-777-0300
Facsimile: 302-777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Jonas McDavit (admitted *pro hac vice*)
Wen Xue (admitted *pro hac vice*)
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
Telephone: 212-351-3400
Facsimile: 212-351-3401
jmcdavit@desmaraisllp.com
wxue@desmaraisllp.com

Attorneys for Plaintiff ZapFraud, Inc.