IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
_____ Division

STRIKEFORCE TECHNOLOGIES, INC., **Plaintiff,** **v.** **ENTRUST, INC., ENTRUST DATACARD CORPORATION, and CYGNACOM SOLUTIONS, INC.,** **Defendants.**	Civil Action No. 1:17-cv-309 (LMB/TCB) **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT AND JURY DEMAND

StrikeForce Technologies, Inc. (hereinafter "Plaintiff" or "StrikeForce") files this Complaint for patent infringement against Entrust, Inc., Entrust Datacard Corporation, and Cygnacom Solutions, Inc. (hereinafter, collectively, "Defendants" or "Entrust") for infringement of U.S. Patent Nos. 8,484,698 and 8,713,701 (collectively, "Asserted Patents"). On personal knowledge as to Plaintiff's own actions, and on information and belief as to the actions of others, Plaintiff alleges as follows:

NATURE OF THE ACTION

1. This is a patent infringement action by StrikeForce to end Entrust's unauthorized and infringing manufacture, use, sale, offering for sale, and/or importation of products and methods in the U.S. incorporating StrikeForce's patented inventions.

2. Plaintiff StrikeForce seeks monetary damages, pre-judgment and post-judgment interest, and injunctive relief for Entrust's past and on-going infringement of the Asserted Patents.

THE PARTIES

3. Plaintiff StrikeForce Technologies, Inc. is a corporation organized and existing under the laws of the State of Wyoming, having its principal place of business located at 1090 King Georges Post Road, Edison, New Jersey 08837.

4. Upon information and belief, defendant Entrust, Inc. is a corporation organized under the laws of the State of Maryland, having its principal place of business located at Three Lincoln Centre, 5430 LBJ Freeway, Suite 1250, Dallas, Texas 75240.

5. Upon information and belief, defendant Entrust Datacard Corporation is a corporation organized under the laws of the State of Delaware, having its principal place of business located at 1187 Park Place, Shakopee, Minnesota 55379.

6. Upon information and belief, defendant Entrust Datacard Corporation is the parent corporation of Entrust, Inc.

7. Upon information and belief, defendant Cygnacom Solutions is a corporation organized under the laws of the State of Texas, having its principal place of business located at 7925 Jones Branch Drive, Suite 5200, McLean, Virginia 22102.

8. Upon information and belief, defendant Cygnacom Solutions, Inc. is a wholly owned subsidiary of Entrust, Inc.

JURISDICTION AND VENUE

9. This is a civil action for patent infringement arising under the patent laws of the United States, Title 35, United States Code §§ 1, *et seq.*

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

11. This Court has personal jurisdiction over Entrust because, upon information and belief, Entrust maintains continuous and systematic contacts and directs its activities at residents of, and has committed acts of infringement in, the Commonwealth of Virginia, including in this District. For example, upon information and belief Entrust maintains an interactive website, https://www.entrust.com/, available to residents of the Commonwealth of Virginia, including residents in this District, wherein users of the website can purchase and/or request Entrust products, including its infringing "IdentityGuard" and "Authentication Cloud Service" products. Upon information and belief, Entrust also makes available mobile applications available for download to residents of the Commonwealth of Virginia, including residents in this District, including Entrust's "IdentityGuard Mobile" and "IdentityGuard Mobile Smart Credential" applications.

12. In addition, upon information and belief, Defendant Cygnacom Solutions, Inc. ("Cygnacom") resides in this District and Entrust maintains continuous and systematic contacts, and has a regular and established place of business, through Cygnacom, located at 7925 Jones Branch Drive, Suite 5200 and/or Suite 5400, McLean, Virginia 22102, which "continues to support the Entrust Datacard team" and which is listed on Entrust's website as one of Entrust's "Regional Offices." *See* http://www.cygnacom.com/about.html (last visited Mar. 17, 2017); https://www.entrust.com/contact/locations/#usa (last visited Mar. 17, 2017). Upon information and belief, Entrust maintains employees at the Cygnacom office who provide sales and technical support for Entrust products, including "IdentityGuard" and/or "Authentication Cloud Services" products.

13. Upon information and belief, Entrust also maintains continuous and systematic contacts with this District through its "partner" ePlus Technology Inc., located at 13595 Dulles Technology Drive, Herndon, VA 20171. *See* https://www.entrustdatacard.com/edc-partners/eplus-technology-inc/ (last visited Mar. 17, 2017).

14. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(a)-(c) and 1400(b).

JOINDER

15. Upon information and belief, the right to relief asserted against Defendants in this Complaint arises out of the same transaction, occurrence, or series of transactions or occurrences relating to the making, using, selling, offering for sale, and/or importing in the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the Asserted Patents. Therefore, questions of fact common to all Defendants will arise in this action and joinder of Defendants under 35 U.S.C. § 299 is proper.

STRIKEFORCE OUT-OF-BAND PATENTS AND PRODUCTS

16. U.S. Patent No. 8,484,698 (the "'698 patent"), titled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)," was duly and legally issued on July 9, 2013. StrikeForce Technologies, Inc. is the owner by assignment of all right, title, and interest in and to the '698 patent, including without limitation the right to sue and recover for past, current, and future infringement thereof. A copy of the '698 patent is attached as Exhibit A to this Complaint.

17. U.S. Patent No. 8,713,701 (the "'701 patent"), titled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)," was duly and legally issued on April 29, 2014. StrikeForce Technologies, Inc. is the owner by assignment of all right, title, and interest in and to the '701 patent, including without limitation the right to sue and

recover for past, current, and future infringement thereof. A copy of the ’701 patent is attached as Exhibit B to this Complaint.

18. The inventions of the ’698 and ’701 patents are directed to multichannel security systems and methods for authenticating a user seeking to gain access to, for example, Internet websites and VPN networks, such as those used for conducting banking, social networking, business activities, and other online services. This field of technology relates to what is sometimes referred to as “out-of-band” authentication or a type of “two-factor” authentication.

19. StrikeForce offers a product called ProtectID® that performs out-of-band authentication according to the teachings of one or more of the Asserted Patents. StrikeForce has offered this product since August 2003, and ProtectID® has displayed the statutory patent notice for its issued patents at its website, www.strikeforcetech.com, since about February 2011. In particular, StrikeForce’s website identified U.S. Patent No. 7,870,599, to which the Asserted Patents claim priority, at least as early as February 2011; StrikeForce’s website identified the ’698 patent at least as early as October 2013; and StrikeForce’s website identified the ’701 patent at least as early as June 2014.

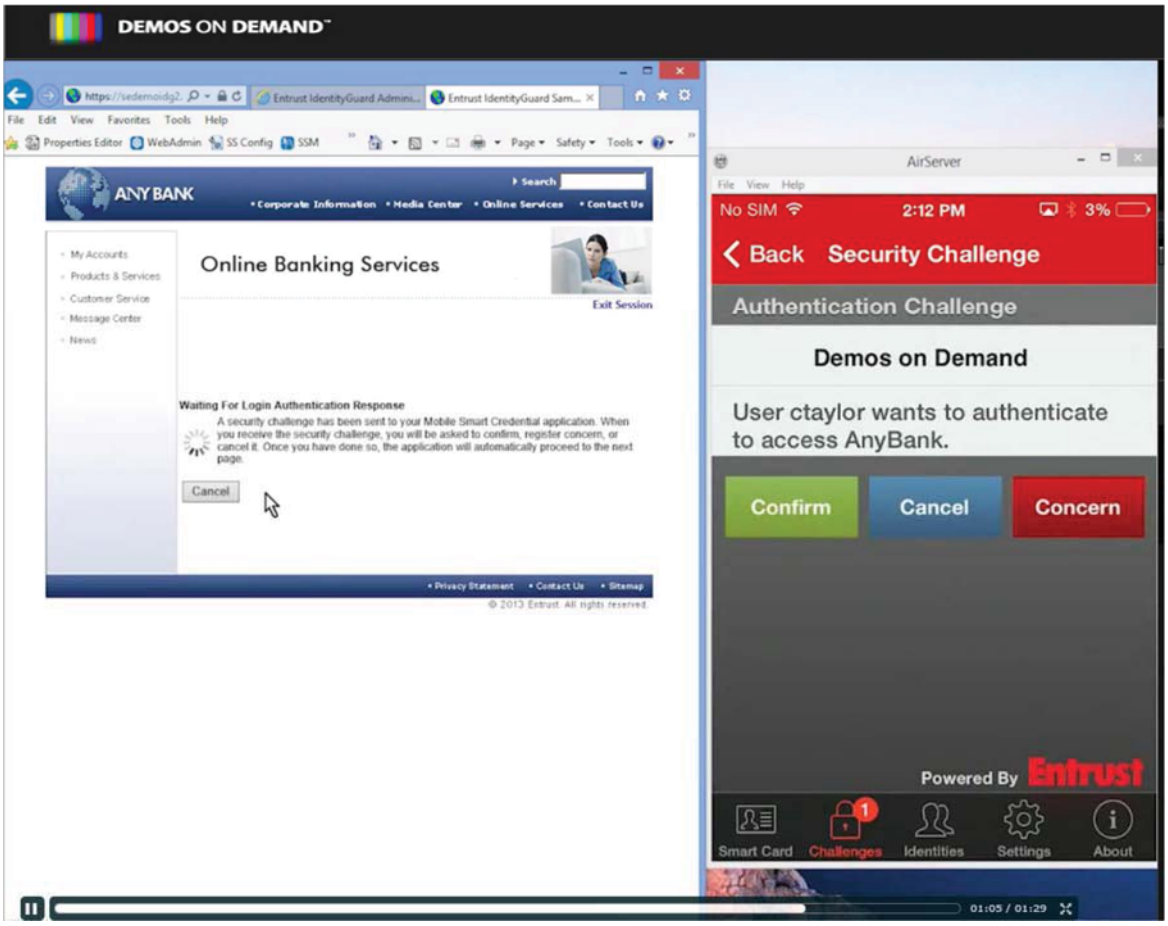
20. Upon information and belief, Entrust has had actual knowledge of the ’698 patent and the ’701 patent at least as early as, and no later than, the filing of this Complaint.

ENTRUST’S INFRINGING PRODUCTS

21. Upon information and belief, Entrust offers two-factor authentication products for use on Android and/or iOS devices in the United States and in this District. These products include, but are not limited to, Entrust IdentityGuard, Entrust IdentityGuard Mobile, Entrust IdentityGuard Virtual Appliance, (collectively, “IdentityGuard Products”) and Entrust Datacard

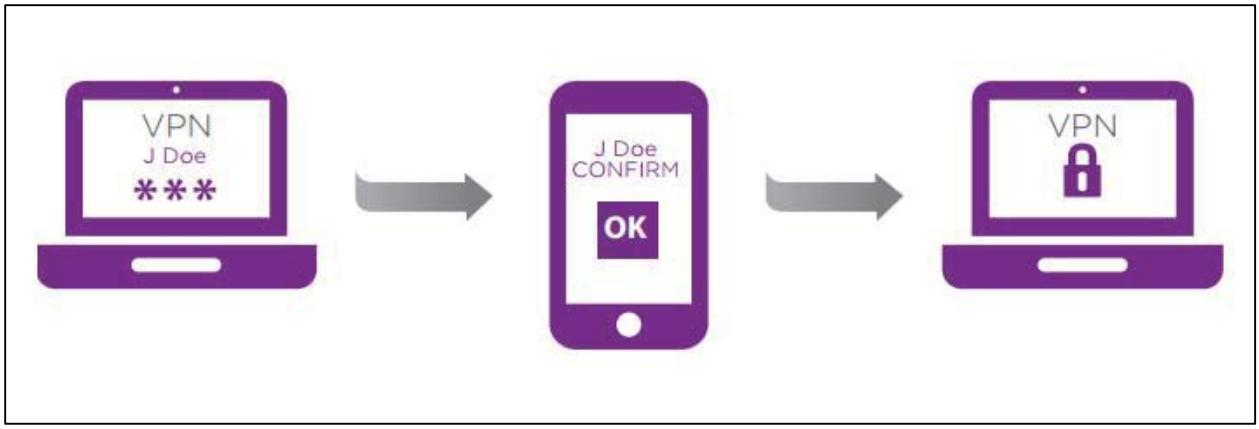
Authentication Cloud Service. *See, e.g.*, https://www.entrust.com/ (under "Products & Services") (last visited Mar. 17, 2017).

22. Upon information and belief, IdentityGuard Products utilize out-of-band technology that sends a notification to a user's device (*e.g.*, through Entrust's Mobile Smart Credential application and/or Entrust's IdentityGuard Mobile application) when a login request is made to provide out-of-band, two-factor authentication with a user's mobile device, such as a smartphone. For example, as Entrust explains in a demonstration video available at http://www.demosondemand.com/html5/?sessID=5109&promotion_id=0&startTime=0&reseller_id=443 (last visited Mar. 17, 2017), "Mobile Smart Credential is an innovative virtual smart card application running on the mobile device…. [that can] receive those security challenges out-of-band in order to prevent having a malware impersonate [the user]….":

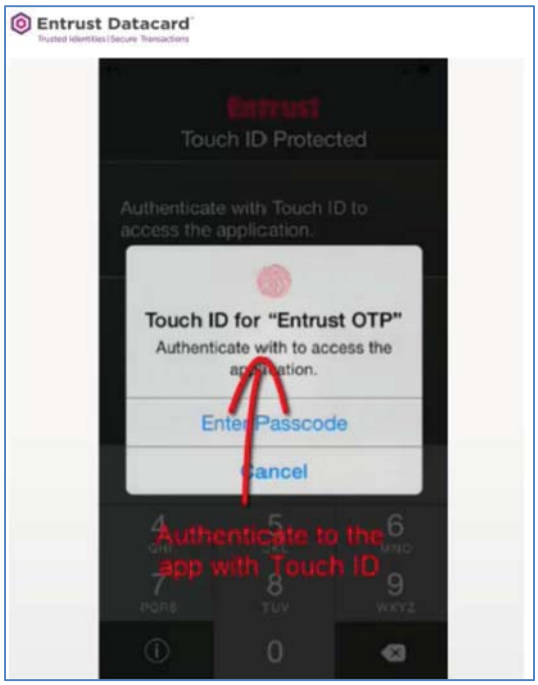


23. Upon information and belief, IdentityGuard and IdentityGuard Mobile comprise systems and/or services that incorporate a server (or servers) ("IdentityGuard Server") for receiving and authenticating requests for access (*e.g.*, through a login attempt) to protected information residing on a computer (or computers), including through website applications. For example, when a user uses a device, such as a computing device, to attempt to access the protected computer or application, such as through the Internet, the user's request for access is directed to the IdentityGuard Server. The IdentityGuard Server retrieves information about the user from a database, such as a phone number or address of the user's mobile device, and sends a "push" notification out-of-band to the user's mobile device, requesting authorization for the access request.

24. Upon information and belief, when the push notification arrives on the user's mobile device, the user is prompted to open a previously downloaded Entrust mobile application to see the details of the authorization request. The user is then prompted to respond to the login request by transmitting a response using Entrust's mobile application running on the user's mobile device to either confirm or deny the request. The user's response is delivered to the IdentityGuard Server through an out-of-band channel. Once the user's response is validated by the IdentityGuard Server, the requested access to the protected computer or application will be granted. *See, e.g.*, Exhibit C; Exhibit G; Exhibit H; Exhibit I; Exhibit J. An exemplary diagram showing this process, in Exhibit C, available at https://www.entrust.com/wp-content/uploads/2015/04/DS-IDG-Mobile-Push-Auth-FEB16-WEB3.pdf (last visited Mar. 17, 2017), is reproduced below:

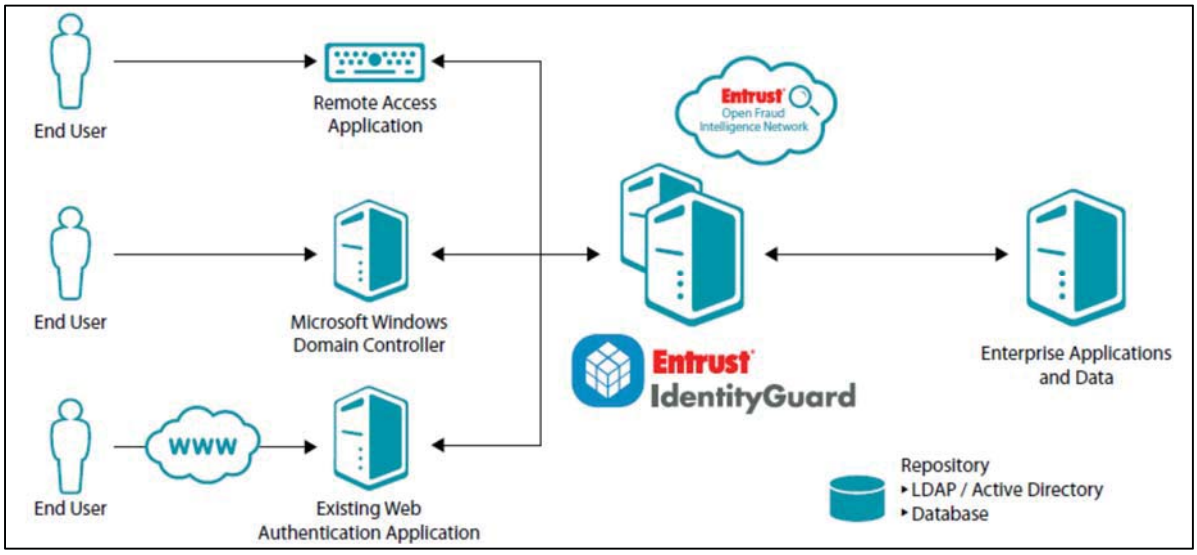


25. Upon information and belief, IdentityGuard and IdentityGuard Mobile also incorporate authentication functionality using biometric data and analysis. For example, when a push notification arrives on the user's mobile device, the user is prompted to open a previously downloaded Entrust mobile application to see the details of the authorization request. The user may be asked to input biometric data, *e.g.*, by scanning his or her fingerprint in order to open the Entrust mobile application as an additional layer of authentication. *See, e.g.*, Exhibit C at 3; Exhibit J at 5. An exemplary screenshot of this feature is reproduced below (*see* Exhibit J at 5):



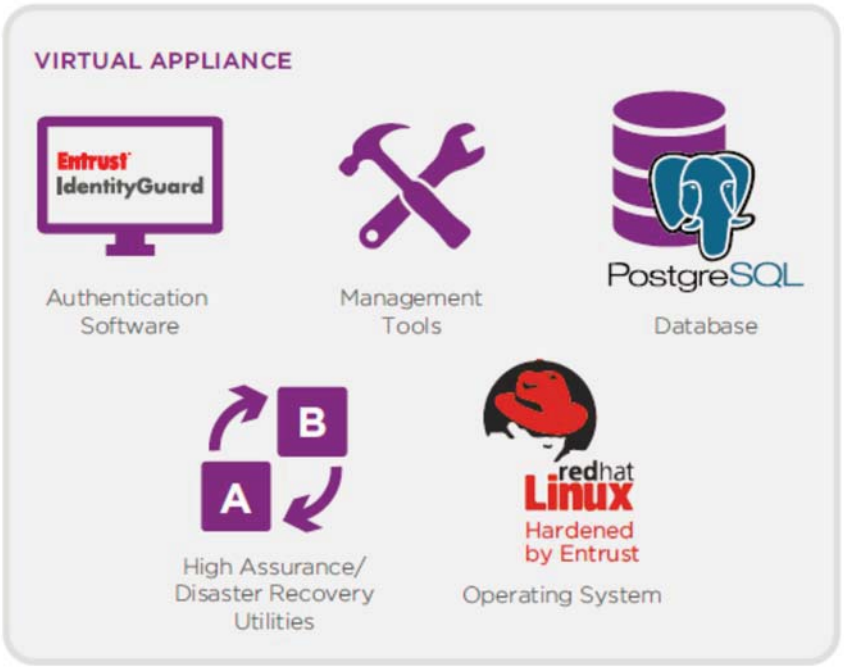
26. In addition, upon information and belief, IdentityGuard and IdentityGuard Mobile incorporate a fingerprint verification program that authenticates a user based on a comparison of a user's stored fingerprint data, wherein an "encrypted mathematical representation . . . [of a user's fingerprint] is compared to the actual fingerprint provided at the time of authentication." Exhibit L at 2; *see also, e.g.*, *id.* at 1–2; Exhibit M at 2–3; Exhibit N at 1-2.

27. An exemplary diagram illustrating the IdentityGuard system, in Exhibit I, available at https://www.entrust.com/wp-content/uploads/2013/05/DS_IDG10-1-ENT_web_Feb2012.pdf (last visited Mar. 17, 2017), is reproduced below:



28. Upon information and belief, the Entrust IdentityGuard Virtual Appliance ("Virtual Appliance") similarly utilizes out-of-band technology that sends a notification to the user's mobile device when a login request is made to provide two-factor authentication with, *e.g.*, a mobile phone. Entrust IdentityGuard Virtual Appliance is a two-factor authentication solution that includes an operating system, database, and management tools, among other things, as illustrated in the graphic below, from Exhibit D, available at https://www.entrust.com/wp-

content/uploads/2016/04/Entrust-IdentityGuard-Virtual-Appliance-SB-OCT16-WEB3.pdf (last visited Mar. 17, 2017):



29. Upon information and belief, Virtual Appliance utilizes out-of-band mobile push authentication sent from a server ("Virtual Appliance Server") to authorize a user's login request prior to granting access to a protected computer or application in the same or a similar way as IdentityGuard and IdentityGuard Mobile. *See, e.g.*, Exhibit D; Exhibit H; Exhibit J.

30. Upon information and belief, the Entrust Datacard Authentication Cloud Service ("Cloud Service") similarly utilizes out-of-band technology in the "cloud" (*i.e.*, over the Internet) that sends a notification to the user's mobile device when a login request is made to provide two-factor authentication with, *e.g.*, a mobile phone. Cloud Service is designed to integrate with Entrust's clients' existing network and protected computers and applications to provide a cloud-based authentication service. Upon information and belief, Cloud Service utilizes out-of-band mobile push authentication sent from a server ("Cloud Server") to authorize a user's login

request prior to granting access to a protected computer or application in the same or a similar way as IdentityGuard and IdentityGuard Mobile. *See, e.g.*, Exhibit E; Exhibit F; Exhibit H; Exhibit J.

31. An exemplary diagram illustrating the Cloud Service system structure, in Exhibit E, available at https://www.entrust.com/wp-content/uploads/2016/06/Entrust-Authentication-Cloud-Service_SB_JUN16_WEB2.pdf (last visited Mar. 17, 2017), is reproduced below (the Entrust logo is within the cloud graphic):

COUNT I –INFRINGEMENT OF THE '698 PATENT

32. StrikeForce incorporates by reference the averments set forth in paragraphs 1 through 31.

33. Pursuant to 35 U.S.C. § 271(a), Entrust has directly infringed, and continues to directly infringe the '698 patent by making, using, selling, offering for sale, and/or importing in

the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the ’698 patent, including, but not limited to, systems, services, and/or software incorporating or implementing Entrust IdentityGuard, Entrust IdentityGuard Mobile, Entrust IdentityGuard Virtual Appliance, and Entrust Datacard Authentication Cloud Service, including mobile applications working in conjunction therewith such as Entrust’s Mobile Smart Credential application and/or Entrust’s IdentityGuard Mobile application (collectively, the “Accused Products”). Entrust thereby directly infringes one or more claims of the ’698 patent, including at least claim 1 of the ’698 patent. Entrust directly infringes at least through its own activities in making, using (including through testing), selling, offering for sale, and/or importing the Accused Products as well as, to the extent applicable, jointly with activities of others under the direction and control of Entrust, including customers of Entrust and/or distributors and “partners” who sell and offer to sell the Accused Products.

34. Upon information and belief, and as demonstrated by the allegations above and the supporting exhibits to this Complaint, the Accused Products satisfy each and every element of one or more claims of the ’698 patent, including, and without limitation, at least claim 1 of the ’698 patent.

35. For example, and without limitation, the Accused Products comprise a software method for employing a multichannel security system to control access to a computer (*e.g.*, software-based authentication platform of the IdentityGuard Products and Cloud Service). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 3–4; Exhibit E at 2–3; Exhibit F at 1–2; Exhibit G at 9; Exhibit H at 1–6; Exhibit I at 1. The Accused Products receive at an interception device in a first channel a login identification demand to access a host computer also in the first channel (*e.g.*, an element of the system that intercepts the user’s login request prior to granting access to the

protected information in, for example, the computer or application). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 3–4; Exhibit E at 2–3; Exhibit H at 2–3; Exhibit I at 4; Exhibit K at 7. The Accused Products verify the login identification (*e.g.*, by verifying the login information of the user). *See, e.g.*, *id.* The Accused Products receive at a security computer in a second channel (*e.g.*, Entrust IdentityGuard Server, Virtual Appliance Server, or Cloud Server) the demand for access and the login identification and output a prompt requesting transmission of data (*e.g.*, push notification to user's mobile device requesting user to confirm or deny authorization). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 2; Exhibit E at 2–3; Exhibit F at 2; Exhibit G at 9; Exhibit H at 3–4; Exhibit I at 4; Exhibit J at 4; Exhibit K at 7. The Accused Products receive the transmitted data at the security computer compare the transmitted data to predetermined data and depending on the comparison of the transmitted and the predetermined data, output an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto (*e.g.*, Entrust IdentityGuard Server, Virtual Appliance Server, or Cloud Server receives the user's response and outputs an instruction to the protected computer to grant or deny access to the requested protected computer or application based on that response). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 2; Exhibit E at 2–3; Exhibit H at 4–6; Exhibit I at 4; Exhibit J at 6–7; Exhibit K at 7–8.

36. Under 35 U.S.C. § 271(b), Entrust has indirectly infringed and continues to indirectly infringe the '698 patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the Accused Products. Entrust distributes, markets, and/or advertises the Accused Products in this District and elsewhere in the United States, including through at least Entrust's website and online demonstrations of its products. *See, e.g.*, Exhibits C–N.

37. Upon information and belief, with knowledge of the ’698 patent and its infringement thereof, Entrust distributes its marketing materials and advertisements, and provides support for installing and implementing the Accused Products, to knowingly instruct and direct users/customers to use the Accused Products in an infringing manner.

38. Under 35 U.S.C. § 271(c), with knowledge of the ’698 patent and its infringement thereof, Entrust has indirectly infringed, and continues to indirectly infringe the ’698 patent by, *inter alia*, knowingly providing to its customers the Accused Products, which constitute material components of an infringing out-of-band authentication system/service and that was especially made or adapted for use in that system, which are not staple articles or commodities of commerce and which have no substantial, non-infringing use. *See, e.g.*, Exhibit D at 2; Exhibit E at 2–3; Exhibit F at 2; Exhibit I at 3–4.

39. Entrust puts the Accused Products into service and exercises control over said systems.

40. Entrust had and/or has knowledge of the ’698 patent and its infringement thereof at least as early as the filing of this Complaint.

41. Entrust’s customers directly infringe one or more claims of the ’698 patent by, for example, integrating the claimed systems and methods, including at least claim 1, directly into the customers’ web services and/or existing protected access control systems and directly benefitting from the use of those services and/or systems. For example, Entrust’s customers in the United States utilize the two-factor authentication systems and methods claimed in the ’698 patent, including at least claim 1, for the purpose of gaining secure access to, exemplarily, various Internet websites and other secure networks.

42. Upon information and belief, Entrust knowingly provides its customers with products and web services that are used in a manner that infringes one or more claims of the ’698 patent, including at least claim 1, as illustrated exemplarily above in paragraph 35.

43. Upon information and belief, through its marketing activities, instructions and directions, and through the sales and offers for sale of infringing systems and methods, Entrust specifically intends for, and/or specifically encourages and instructs, its customers to use its products and web services and knows that its customers are using its products and web services in an infringing manner.

44. As a direct and proximate result of Entrust’s acts of infringing one or more claims of the ’698 patent, StrikeForce has suffered injury and monetary damages for which StrikeForce is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for Entrust’s infringement.

45. Entrust will continue to directly infringe one or more claims of the ’698 patent, causing immediate and irreparable harm to StrikeForce unless this Court enjoins and restrains Entrust’s activities, specifically the acts of making, using, selling, and offering for sale, as previously outlined. There are inadequate remedies available at law to compensate for this harm.

46. Upon information and belief, Entrust’s past and ongoing infringement of the ’698 patent has been and continues to be with full knowledge of the ’698 patent and Entrust’s infringement thereof, at least as of the filing date of this Complaint. Entrust’s knowing, willful, and deliberate infringement of one or more claims of the ’698 patent, including at least claim 1, in conscious disregard of StrikeForce’s rights makes this case exceptional within the meaning of 35 U.S.C. § 285 and justifies treble damages pursuant to 35 U.S.C. § 284.

COUNT II –INFRINGEMENT OF THE '701 PATENT

47. StrikeForce incorporates by reference the averments set forth in paragraphs 1 through 46.

48. Pursuant to 35 U.S.C. § 271(a), Entrust has directly infringed, and continues to directly infringe the '701 patent by making, using, selling, offering for sale, and/or importing in the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the '701 patent, including, but not limited to, the Accused Products. Entrust thereby directly infringes one or more claims of the '701 patent, including at least claim 1 of the '701 patent. Entrust directly infringes at least through its own activities in making, using (including through testing), selling, offering for sale, and/or importing the Accused Products as well as, to the extent applicable, jointly with activities of others under the direction and control of Entrust, including customers of Entrust and/or distributors and "partners" who sell and offer to sell the Accused Products.

49. Upon information and belief, and as demonstrated by the allegations above and the supporting exhibits to this Complaint, the Accused Products satisfy each and every element of one or more claims of the '701 patent, including, and without limitation, at least claim 1 of the '701 patent.

50. For example, and without limitation, the Accused Products comprise a security system for accessing a host computer (*e.g.*, software-based authentication platform of the IdentityGuard Products and Cloud Service). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 3–4; Exhibit E at 2–3; Exhibit F at 1–2; Exhibit G at 9; Exhibit H at 1–6; Exhibit I at 1. The Accused Products include an access channel comprising an interception device for receiving a login identification originating from an accessor for access to said host computer (*e.g.*, an element of

the system that intercepts the user's login request prior to granting access to the protected information in, for example, the computer or application). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 3–4; Exhibit E at 2–3; Exhibit H at 2–3; Exhibit I at 4; Exhibit K at 7. The Accused Products include, in an authentication channel, a security computer (*e.g.*, Entrust IdentityGuard Server, Virtual Appliance Server, or Cloud Server) for receiving from said interception device said login identification and for communicating access information to said host computer and for communicating with a peripheral device of said accessor (*e.g.*, push notification to user's mobile device requesting user to confirm or deny authorization). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 2; Exhibit E at 2–3; Exhibit F at 2; Exhibit G at 9; Exhibit H at 3–4; Exhibit I at 4; Exhibit J at 4; Exhibit K at 7. The Accused Products include a database having at least one peripheral address record corresponding to said login identification (*e.g.*, database accessed by IdentityGuard Server, Virtual Appliance Server, or Cloud Server for communicating with the user's mobile device). *See, e.g.*, Exhibit D at 3; Exhibit E at 3; Exhibit I at 4. The Accused Products include, in an authentication channel, a prompt mechanism for instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device (*e.g.*, an element of the system that issues a push notification on the user's mobile device prompting the user to confirm or deny authorization). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 2; Exhibit E at 2; Exhibit F at 2; Exhibit G at 9; Exhibit H at 3–4; Exhibit J at 4. The Accused Products include, in an authentication channel, a comparator for authenticating access demands in response to the transmission of said predetermined data by verifying a match between said predetermined data and said entered and transmitted data, wherein said security computer outputs an instruction to the host computer to either grant access thereto using said access channel or to deny access thereto (*e.g.*, Entrust IdentityGuard Server, Virtual Appliance Server,

or Cloud Server receives the user's response and outputs an instruction to the protected computer to grant or deny access to the requested protected computer or application based on that response). *See, e.g.*, Exhibit C at 1–2; Exhibit D at 2; Exhibit E at 2–3; Exhibit H at 4–6; Exhibit I at 4; Exhibit J at 6–7; Exhibit K at 7–8.

51. Under 35 U.S.C. § 271(b), Entrust has indirectly infringed and continues to indirectly infringe the '701 patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the Accused Products. Entrust distributes, markets, and/or advertises the Accused Products in this District and elsewhere in the United States, including through at least Entrust's website and online demonstrations of its products. *See, e.g.*, Exhibits C–N.

52. Upon information and belief, with knowledge of the '701 patent and its infringement thereof, Entrust distributes its marketing materials and advertisements, and provides support for installing and implementing the Accused Products, to knowingly instruct and direct users/customers to use the Accused Products in an infringing manner.

53. Under 35 U.S.C. § 271(c), with knowledge of the '701 patent and its infringement thereof, Entrust has indirectly infringed, and continues to indirectly infringe the '701 patent by, *inter alia*, knowingly providing to its customers the Accused Products, which constitute material components of an infringing out-of-band authentication system/service and that was especially made or adapted for use in that system, which are not staple articles or commodities of commerce and which have no substantial, non-infringing use. *See, e.g.*, Exhibit D at 2; Exhibit E at 2–3; Exhibit F at 2; Exhibit I at 3–4.

54. Entrust puts the Accused Products into service and exercises control over said systems.

55. Entrust had and/or has knowledge of the ’701 patent and its infringement thereof, at least as early as the filing of this Complaint.

56. Entrust’s customers directly infringe one or more claims of the ’701 patent by, for example, integrating the claimed systems and methods, including at least claim 1, directly into the customers’ web services and/or existing protected access control systems and directly benefitting from the use of those services and/or systems. For example, Entrust’s customers in the United States utilize the two-factor authentication systems and methods claimed in the ’701 patent, including at least claim 1, for the purpose of gaining secure access to, exemplarily, various Internet websites and other secure networks.

57. Upon information and belief, Entrust knowingly provides its customers with products and web services that are used in a manner that infringes one or more claims of the ’701 patent, including at least claim 1, as illustrated exemplarily above in paragraph 50.

58. Upon information and belief, through its marketing activities, instructions and directions, and through the sales and offers for sale of infringing systems and methods, Entrust specifically intends for, and/or specifically encourages and instructs, its customers to use its products and web services and knows that its customers are using its products and web services in an infringing manner.

59. As a direct and proximate result of Entrust’s acts of infringing one or more claims of the ’701 patent, StrikeForce has suffered injury and monetary damages for which StrikeForce is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for Entrust’s infringement.

60. Entrust will continue to directly infringe one or more claims of the ’701 patent, causing immediate and irreparable harm to StrikeForce unless this Court enjoins and restrains

Entrust's activities, specifically the acts of making, using, selling, and offering for sale, as previously outlined. There are inadequate remedies available at law to compensate for this harm.

61. Upon information and belief, Entrust's past and ongoing infringement of the '701 patent has been and continues to be with full knowledge of the '701 patent and Entrust's infringement thereof, at least as of the filing date of this Complaint. Entrust's knowing, willful, and deliberate infringement of one or more claims of the '701 patent, including at least claim 1, in conscious disregard of StrikeForce's rights makes this case exceptional within the meaning of 35 U.S.C. § 285 and justifies treble damages pursuant to 35 U.S.C. § 284.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Entrust as follows:

A. Declaring that the '698 patent was duly and legally issued, and is valid and enforceable;

B. Declaring that the '701 patent was duly and legally issued, and is valid and enforceable;

C. Declaring that Entrust has infringed the '698 patent;

D. Declaring that Entrust has willfully infringed the '698 patent;

E. Declaring that Entrust has infringed the '701 patent;

F. Declaring that Entrust has willfully infringed the '701 patent;

G. Awarding to Plaintiff damages caused by Entrust's infringement, including all lost profits resulting from Entrust's acts of infringement, and in no event less than reasonable royalties, together with pre-judgment and post-judgment interest and supplemental damages for any continuing post-verdict infringement up until entry of the final judgment, with an accounting, as needed, pursuant to 35 U.S.C. § 284;

H. Awarding to Plaintiff treble damages for infringement of the ’698 and ’701 patents as a consequence of Entrust’s willful infringement;

I. Enjoining Entrust, its officers, agents, servants, employees, attorneys, all parent and subsidiary corporations and affiliates, its assigns and successors in interest, and those persons in active concert or participation with Entrust who receive notice of the injunction, from continuing acts of infringement of the ’698 and ’701 patents;

J. Ordering that, in the event a permanent injunction preventing future acts of infringement is not granted, Plaintiff be awarded a compulsory ongoing license fee;

K. Adjudging this an exceptional case and awarding to Plaintiff its reasonable attorneys’ fees pursuant to 35 U.S.C. § 285; and

L. Awarding to Plaintiff such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to Rule 38(b), Fed. R. Civ. P., Plaintiff demands a trial by jury on all of the claims so triable.

Dated: March 17, 2017

Respectfully submitted,

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Richard T. McCaulley, Jr. (*pro hac vice to be filed*)
ROPES & GRAY LLP
191 North Wacker Drive
32nd Floor
Chicago, IL 60606
Telephone: (312) 845-1200

Steven Pepe (*pro hac vice to be filed*)
Kevin J. Post (*pro hac vice to be filed*)
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
Telephone: (212) 596-9000

Matthew J. Rizzolo (*pro hac vice to be filed*)
ROPES & GRAY LLP
2099 Pennsylvania Ave, NW
Washington, DC 20006
Telephone: (202) 508-4600

Attorneys for Plaintiff StrikeForce Technologies, Inc.