IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SUNSTONE INFORMATION DEFENSE, INC., Plaintiff, v. INTERNATIONAL BUSINESS MACHINES CORPORATION, Defendant.	CIVIL ACTION NO. 6:20-cv-01033-ADA **JURY TRIAL REQUESTED**

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff SunStone Information Defense, Inc. ("SunStone" or "Plaintiff") files this Amended Complaint for Patent Infringement of U.S. Patent No. 9,122,870 (the "'870 Patent") and U.S. Patent No. 10,958,682 (the "'682 Patent") against Defendant International Business Machines Corporation ("IBM").

IBM Security's Trusteer products and services infringe SunStone's seminal cybersecurity '870 Patent as well as the recently issued '682 Patent.

THE PARTIES

1. SunStone Information Defense, Inc., ("SunStone" or "Plaintiff") is a corporation organized and existing under the laws of the state of Delaware and located at 4 SW 5th Perry Newberry, Carmel, California, 93921.

2. International Business Machines Corporation ("IBM" or "Defendant") is a New York corporation, with its corporate headquarters at 1 New Orchard Road, Armonk, New York 10504.

3. IBM is registered to do business in Texas and may be served through its registered agent, CT Corporation System, at 1999 Bryan St., Ste. 900, Dallas TX 75201-3136.

JURISDICTION AND VENUE

4. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq*., including, without limitation, 35 U.S.C. §§ 154, 271, 281, 283-285.

5. IBM maintains a permanent physical presence within the Western District of Texas and regular and established places of business within the district at its IBM research facility located at 11501 Burnet Road, Austin, TX 78758.

6. IBM has maintained operations in this District since 1967 and currently employs approximately 6,000 workers in the District.

7. IBM offers to sell, sells, and advertises products and services in this judicial district.

8. IBM advertises, offers to sell, and has sold infringing products, like IBM Security Trusteer Pinpoint Detect ("Trusteer Pinpoint Detect") and IBM

Security Trusteer Mobile ("Trusteer Mobile"), into the stream of commerce knowing or understanding that such products would be used in the United States, including in the Western District of Texas.

9. This Court has personal jurisdiction over IBM. IBM recently admitted to personal jurisdiction and venue in this Court. *De La Vega v. International Business Machines, Corp*., Case No. 6:19-cv-00614, Dkt. No. 22, (W.D. Tex. 2019).

10. IBM has used Trusteer Pinpoint Detect and Trusteer Mobile in the Western District of Texas.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1400(b) on the grounds that IBM has committed acts of infringement in the district and has a regular and established place of business in the district.

SUNSTONE

12. SunStone was founded in 2011 by Dr. David Ford.

13. Dr. Ford is a leading expert in the application of information theory and mathematics to real world problems in computer security. Dr. Ford received a Master of Science in Theoretical and Applied Mechanics from Cornell, and a PhD in Applied Mathematics from the University of Illinois. Dr. Ford is a six-year veteran of the National Security Agency ("NSA") and a graduate of the NSA's three-year Postdoctoral cryptographic program. While at the NSA, Dr. Ford led a team of 50 cyber security experts to field groundbreaking technology. Following the NSA,

Dr. Ford was the Chief Scientist for Information Assurance for DISA at the Naval Postgraduate School ("NPS"). Subsequently, Dr. Ford joined the NPS faculty.

14. Dr. Ford has consulted for a variety of organizations such as the Department of Commerce, the Critical Infrastructure Assurance Office, the eCrimes Task Force in NYC, and the Taliban Sanctions Committee at the United Nations.

15. Dr. Ford is a leading expert in the application of information theory and mathematics to computer security.

16. SunStone is a cybersecurity provider that offers several products for the rapidly developing cyberthreat prevention market, including mobile and desktop solutions. SunStone also focuses on mobile cyber protection due to the dramatic shift toward the expanding mobile financing industry.

17. The cybersecurity market is constantly growing as cyber-threats continue to evolve with hackers improving and refining their tactics and expanding their targets. The cybersecurity industry has grown rapidly in recent years and the mobile transaction market has increased to an estimated value in the hundreds of billions of dollars.

18. Although cybersecurity businesses have been developed, many of these companies focus on two-factor authentication which is neither a cure nor a substantial deterrent; it is merely a minor inconvenience for cyber-attackers.

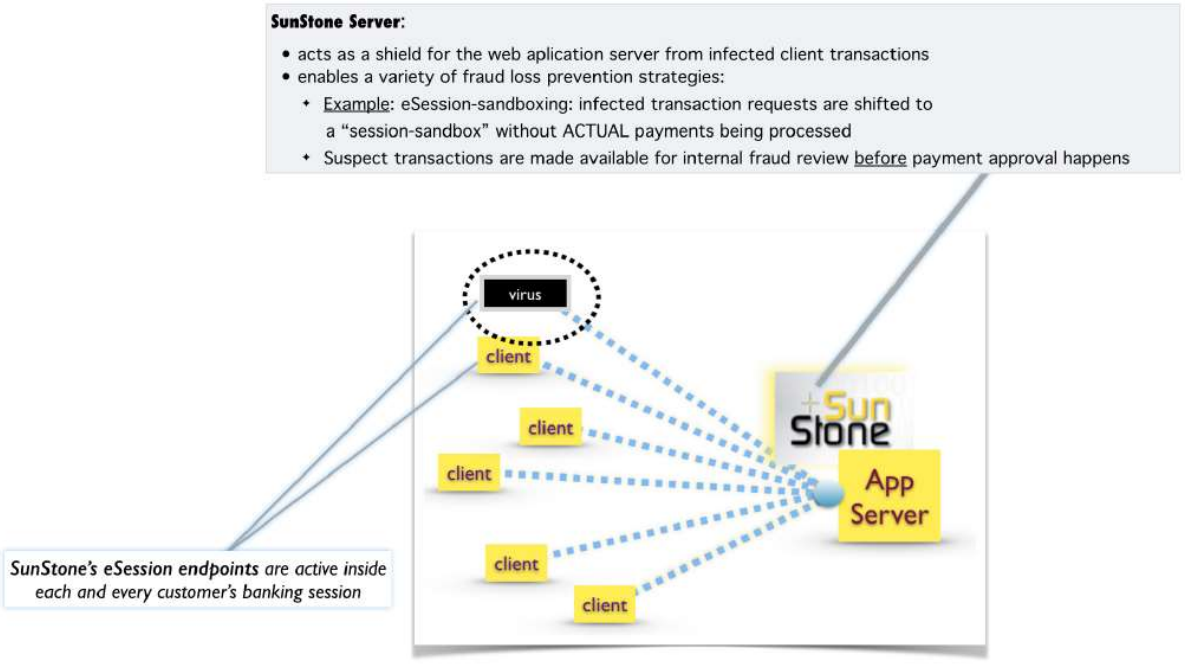
19. SunStone does not offer two-factor authentication. Instead, it offers a much more elaborate and protective service that detects, prevents, and deters cyber-criminals before they achieve their purpose.

20. Some of the most pernicious and difficult to combat cyber-threats are advanced persistent threat viruses, also known as APTs. APTs are the most subtle form of online fraud as they can remain inactive on a device until they detect an active website that is potentially vulnerable. When APTs are not active they are virtually invisible to virus detection software which makes them extremely difficult to safeguard against. Currently, less than 40% of all APTs are detected by organizations, and even fewer are stopped before they can accomplish their purpose.

21. In one type of APT, after the virus has activated it waits patiently until the user has entered all of their information, such as a mobile bank deposit. Once the user confirms the transaction, the virus directs a portion of the information back to the hacker and sends the remaining amount to the bank. The bank responds with an email confirmation showing the new deposit less what the APT removed. The virus then changes the bank statement to record the amount that the user initially intended to deposit and sends the altered email back to the client. The client has no idea they just became a victim of cyber-theft, and the APT will continue to exist on the device until it is either found or deactivated.

22. As an attack tool used by hackers and virus manufacturers, the virus polymorphism technique is employed to successfully blast past client-side anti-virus technologies. The tactic worked extremely well and, before SunStone's solution, went largely unimpeded and unanswered by defensive technologies for the last 20 years.

23. SunStone's technology stops powerful APT viruses by taking control of virus polymorphism away from the malware manufacturers, turning the tables, and using polymorphism against the virus. Acting from the vantage point of the web application server (rather than a local executable), SunStone is able to make the operation of each and every client's web session "polymorphic." These programming polymorphisms take place inside the client's device (exactly when and where the virus is active) without changing the customer experience of the web pages and session flow. No adaptation of the web application server is necessary. No permanent client-side download and installation is required.



24. The SunStone technology sits in-between the server and its clients. As web traffic traverses from server to client, SunStone injects logical changes into the behind-the-scenes programming of the web page. What renders on the client endpoint now is actually a web page that has been modified, without detection, from the original. The modified page looks the same to the end user and the business logic and session flow are not altered. There is no download or install required. SunStone's technology is fileless and lives in browser programming memory while the web session is active.

25. SunStone's technology is particularly useful for the banking industry because online banking architectures are constrained to always allow client-server connections for legitimate customers. Under these conditions, firewall, web application firewalls, and intrusion detection systems add very little in terms of fraud

prevention. These technologies were simply never designed to handle "always allow" architectures or the variety and sophistication of today's banking trojan horse viruses.

26. SunStone provides products and services aimed at network and device security. SunStone originated from experiences encountered while providing information security consulting services in Silicon Valley for the banking industry.

27. In the earlier part of this decade, financial trojans horses, such as Zeus and SpyEye were of particular importance. Statistics show that for every 1,000 infection attempts, banking trojan horses such as Zeus and SpyEye succeed 650 times against traditional client-side antivirus programs.

28. SunStone has developed a successful defensive strategy that now serves as the inventive basis for SunStone's patent portfolio. The SunStone library acts from the vantage point of an eBusiness' web application server, crafting custom modifications that blend in with the programmatic terrain (HTML, Cascading Style Sheets (CSS), JavaScript (JS)) at the client, with no client-side download or install because the web session itself is the download. In this way, the page ultimately rendered by the client device is a "polymorph" of the original—as the now-modified page has been redesigned and repackaged to detect malicious activity yet still maintains its original functionality. Over time, these "polymorphs" may be varied,

as required, to keep the burden of analysis on the attacker. This approach has proven to be almost impenetrable to malicious system attacks.

29. SunStone's technology has attracted interest from a variety of industries such as banking, hospitals, and the United States government.

30. SunStone has leveraged its contacts with the United States government. For example, SunStone has had meetings, given presentations, and demonstrated its products and services at Office of the Director of National Intelligence, National Security Agency, Defense Information Systems Agency, Department of Homeland Security, US Secret Service, and Leidos.

31. In 2013, the NSA contracted with SunStone for use of SunStone's products and services. The SunStone implementation at the NSA is the sole commercial embodiment of the '870 Patent.

32. SunStone has over 25 patents and pending patent applications.

33. SunStone continues in business today as a leading innovator in the cybersecurity field.

SUNSTONE'S PATENTS

34. SunStone's patents are seminal patents in the field of cybersecurity directed against virus polymorphism.

35. Autonomous programs known as "bots" enable hackers to take control of many computers at a time and turn them into zombie computers that can spread

viruses, generate spam, and commit other types of online crime, including financial fraud and ad fraud. There are armies of bots creating and operating fake social media accounts, making purchases with stolen credit cards, hijacking in-session banking transactions, viewing and clicking on ads, and creating significant volumes of fake traffic that result in advertising dollars for fraudsters. Initially targeting display ads on computers, these bots are sophisticated and can infect mobile devices and apps.

36. For a human user, a basic web page is a spatially organized layout of forms, input boxes, and buttons. Other items may be on the page, such as advertisements, videos, and instructional text. However, it is primarily through the forms, input boxes, and buttons that an end-user, wanting to engage a web service (banking, ticketing, social media, etc.), communicates their intent to the application server.

37. Hackers, malware, and botnets (a collection of devices each running one or more bots) also wish to avail themselves of (abuse) these online services. SunStone's patented technology exploits the graphical user interface (GUI) in such a way that automated malware is challenged to remain hidden.

38. From a mathematical perspective, a function is simply a list of input-output pairings. The function "output=input + 1" is shorthand for the infinite list (input, output): (0,1), (1,2), (2,3), (3,4), etc. From an engineering perspective, a graphical user interface ("GUI") is a system of interactive visual components for

computer software. A GUI displays objects that convey information, and represent actions that can be taken by the user. The objects change color, size, or visibility when the user interacts with them. GUI includes a collection of hardware pixels; each pixel is assigned a color and perhaps a function to be performed by software running on the computer, such as the operating system ("OS"). The outputs of these functions link to their inputs (*i.e.*, a specified amount of time or particular user interaction). For example, if a user navigates a cursor over a (video) pixel, a sound is made to come out of the speakers when the video plays. As a second example, once a page has fully loaded, a function runs to create a pop-up (a geometrical region of colored pixels) that states "Welcome User." If a GUI is static with fixed rules associated with the user data entry controls (pixel regions), then static and fixed page navigation occurs. The static and fixed environment may be studied and dissected, allowing the construction of broadly applicable, automated scripts that effectively imitate (or in some cases formally navigate) acceptable interaction with these static controls. To combat these attacks, the colors and function assignments of the pixels must not remain fixed or static.

39. On the other hand, the pixel colors and rules cannot be scrambled to the point of incoherence. Otherwise, the user will not recognize the branding of the site or know how to use the GUI to interact with the server to input their user data (*e.g.*, password, wire transfer recipient). So, there is a balance to be struck in keeping the

user's "recognition" of the GUI static BUT changing the colors and rules tied to the pixel sets to frustrate and detect malware. Ultimately the malware must imitate legitimate user navigation of the forms, inputs, and buttons to communicate with (abuse) the online service. The layout, (relative) geometry, and function rules tied to these features are of strategic importance and must enable differentiated page navigation.

40. Constrained changes to the content that preserve user GUI familiarity but provide sufficient differentiation to the foundational layout, (relative) geometry, and function rules of an application's strategic resources and elements can effectively differentiate and define acceptable user navigation paths. Constrained changes meeting these requirements are called defensive polymorphisms.

THE '870 PATENT

41. SunStone is the owner by assignment from the inventor, David Ford, of all right, title, and interest in and to United States Patent Number 9,122,870 (the "'870 Patent"), titled "Method and Apparatus for Validating Communications in an Open Architecture System" including the right to sue for all past, present, and future infringement.

42. Exhibit A is a true and correct copy of the '870 Patent.

43. The '870 Patent issued from U.S. Patent Application No. 13/623,556 filed on September 20, 2012.

44. The ’870 Patent claims priority to Provisional Application No. 61/557,733, filed on November 9, 2011, and Provisional Application No. 61/537,380, filed on September 21, 2011.

45. The United States Patent and Trademark Office issued the ’870 Patent on September 1, 2015, after a full and fair examination.

46. The ’870 Patent is valid and enforceable.

47. The ‘870 Patent is cited on the face of numerous patents by SunStone’s competitors.

48. The ’870 patent is cited on the face of U.S. Patent No. 10,565,287 B2, which is assigned to IBM.

49. The ’870 Patent describes a method for validating communications in an open architecture system.

50. The ’870 Patent describes an apparatus for validating communications in an open architecture system.

51. Claim 1 of the ’870 Patent recites:

A method comprising:

selecting transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device;

selecting presentation information corresponding to the transactional information to transmit from the server to the client device, the

presentation information specifying how the transactional information is to be displayed;

transmitting at least one message including the presentation and transactional information from the server to the client device;

determining a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information specified by the presentation information, and iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device;

receiving the response message from the client device; and responsive to information in the response message not matching the prediction, providing an indication there is a malicious application affecting communications between the server and the client device,

wherein the prediction is further determined based at least in part by at least one of: (a) estimating locations of rendered features and functions as displayed by the client device, (b) estimating locations of rendered page geometry of the features and functions, (c) estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device, (d) estimating a label of the presentation information, (e) estimating a utilization of a codeword set based on the presentation information and transactional information, and (f) estimating a utilization of a codeword set based on actions taken by at least one of the user and the client device.

'870 Patent, Claim 1.

52. The '870 Patent is directed to a novel apparatus and method for validating communications between servers and client devices. As described by the specification, communications between servers and client devices were prone to problems specific to computer communications:

> Using malicious noise, viruses and other types of malicious applications are able to direct a client device (*e.g.*, a receiver) to perform actions that a communicatively coupled server (*e.g.*, a sender) did not originally intend. Additionally, the viruses and malicious applications are able to direct a server to perform actions that communicatively coupled client devices did not originally intend. Conventional virus detection algorithms often fail to detect the malicious nature of the noise because these algorithms are configured to detect the presence of the noise's source rather than the noise itself. The noise generation algorithm (*e.g.*, the code of the malicious application) is relatively easily disguised and able to assume a wide variety of formats. There is accordingly a need to validate communications between servers and client devices in the presence of malicious noise.

'870 Patent at 2:28-42.

53. An example embodiment of the '870 Patent includes a method of selecting transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device, selecting presentation information corresponding to the transactional information to transmit from the server to the client device, transmitting at least one message including the presentation and transactional information from the server to the client device, determining a prediction as to how the client device will render the transactional information based on the presentation information, receiving a response message from the client, and responsive to information in the response message not matching the prediction, providing an indication there is a malicious application affecting communications between the server and the client device.

54. The '870 Patent describes a network communication system that includes one or more client devices, application servers, and database servers connected to one or more databases. Each of the client devices may communicate with one another on the network, such as for example, the Internet or a local area network. The application servers may provide services accessible to the client devices while the database servers provide a framework for the client devices to access data stored in the databases. The application servers can provide, for example, banking services, government services, etc. After selecting which soft and hard information to send to the client device, the security processor makes a prediction, such as, the location of a "Submit" icon on a fully rendered webpage that is part of a banking website provide by the application server. The security processor then monitors responses by the client device to identify coordinates of a mouse click of the "Submit" icon to determine if a malicious application is affecting communications if the prediction does not match the reported coordinates of the mouse click. The security processor would then attempt to prevent the malicious application from further communications with the affected client device.

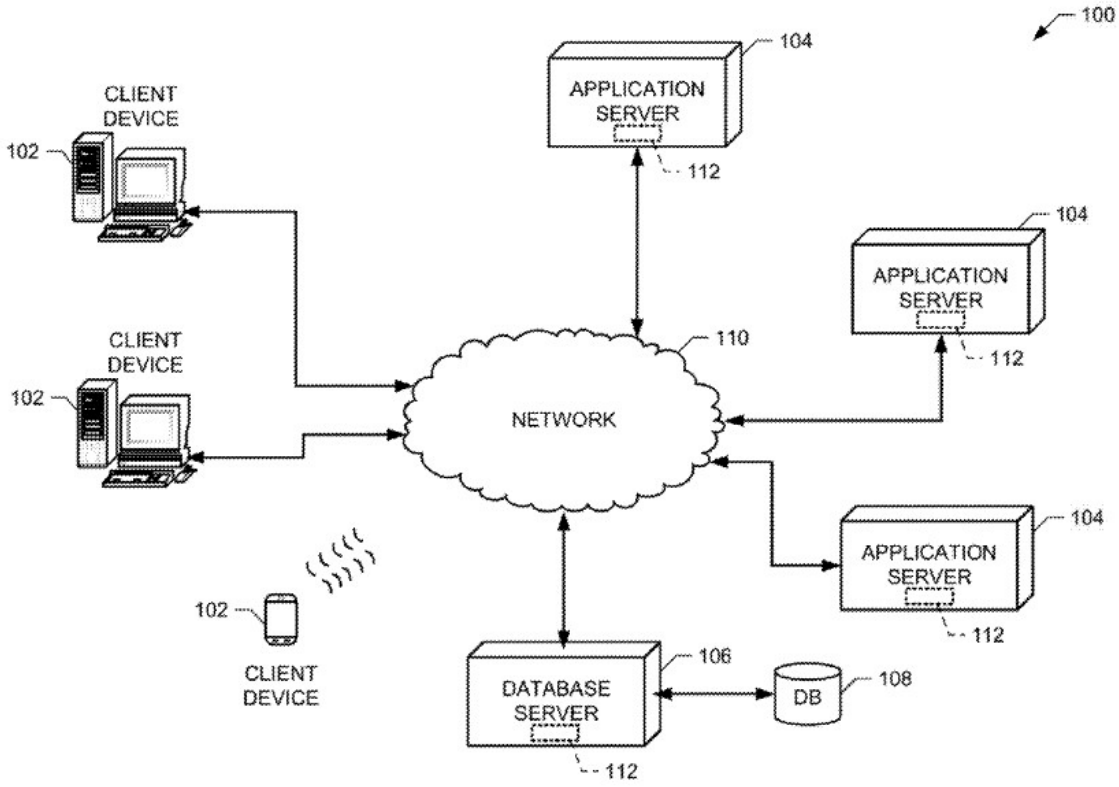


FIG. 1

'870 Patent at Fig. 1.

55. The client devices, application servers, and database servers described above would include computing devices with microprocessors, memory, an interface circuit (which may be implemented using any suitable interface standard, such as, for example, an Ethernet interface and/or a Universal Serial Bus (USB) interface), and storage devices such as a hard drive.

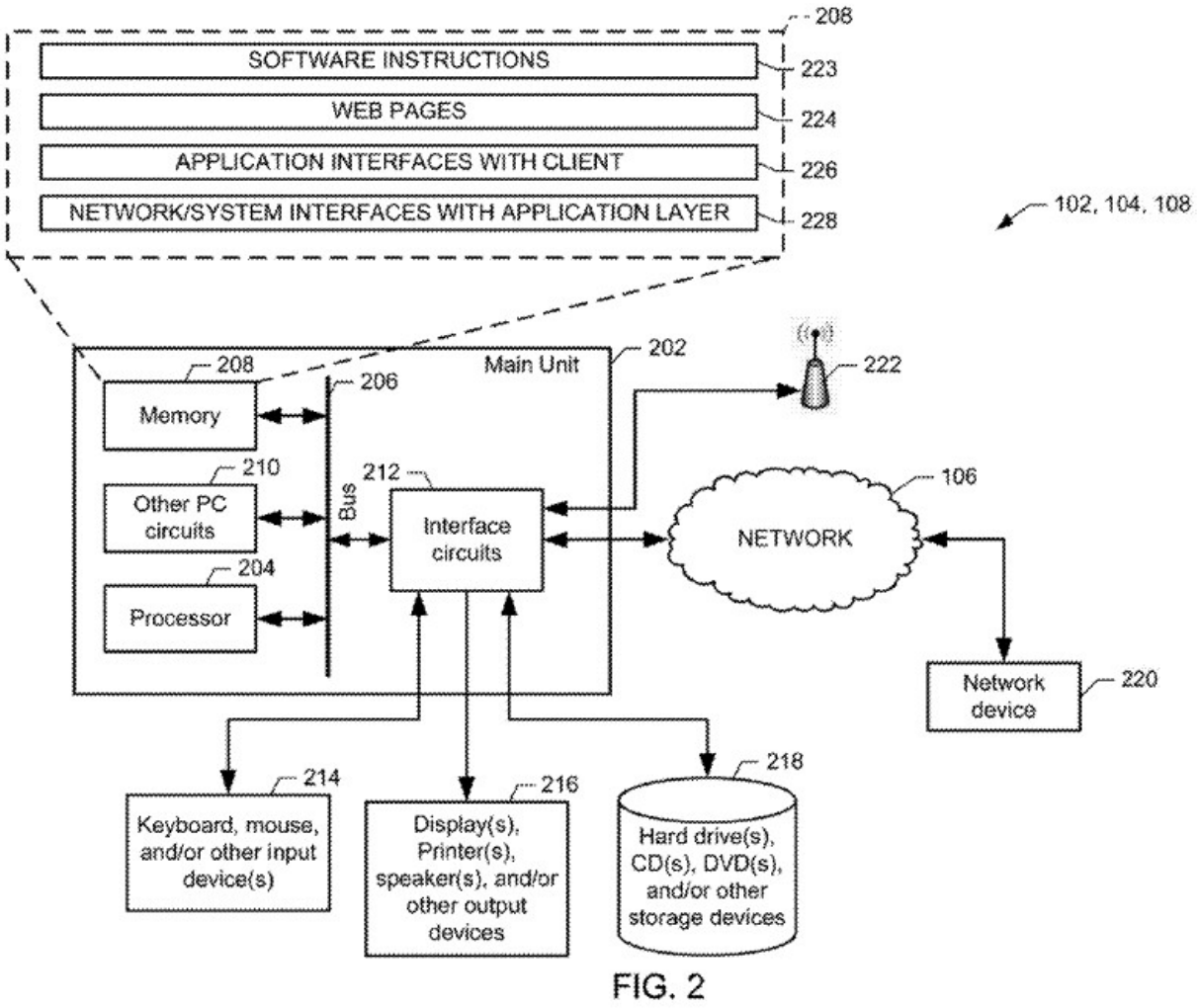


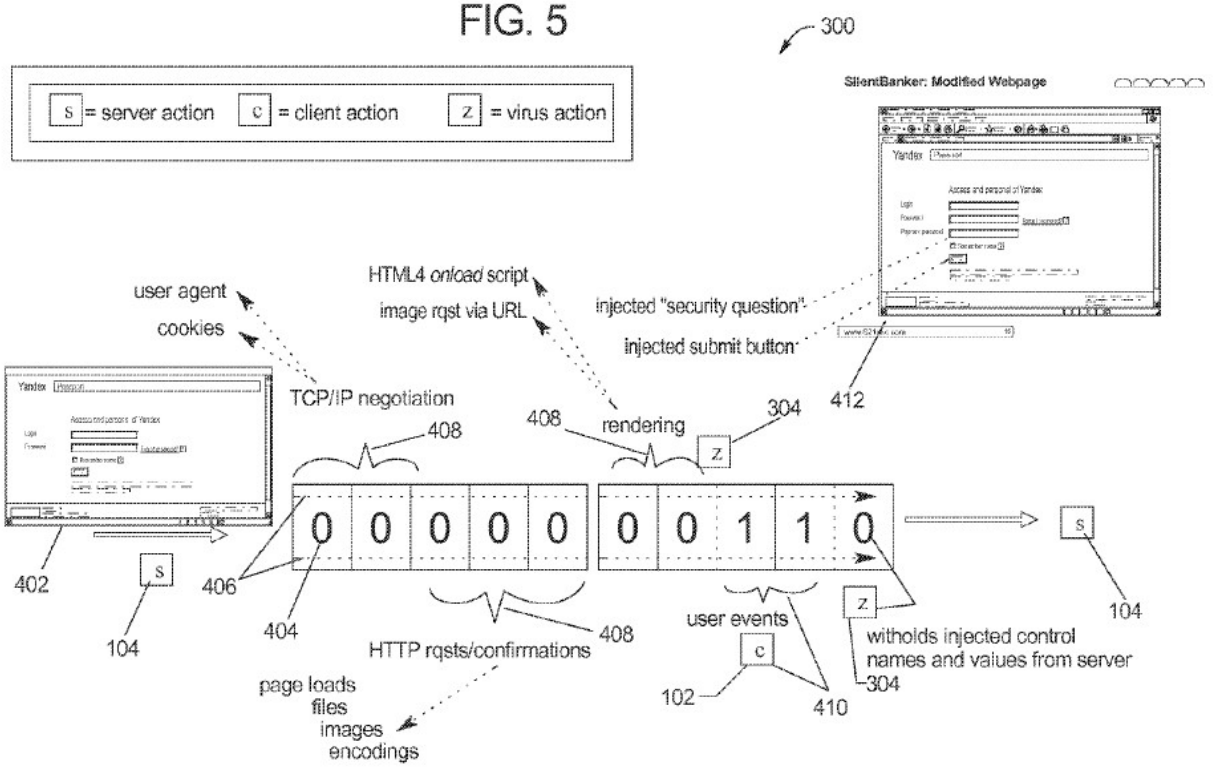
FIG. 2

'870 Patent at Fig. 2.

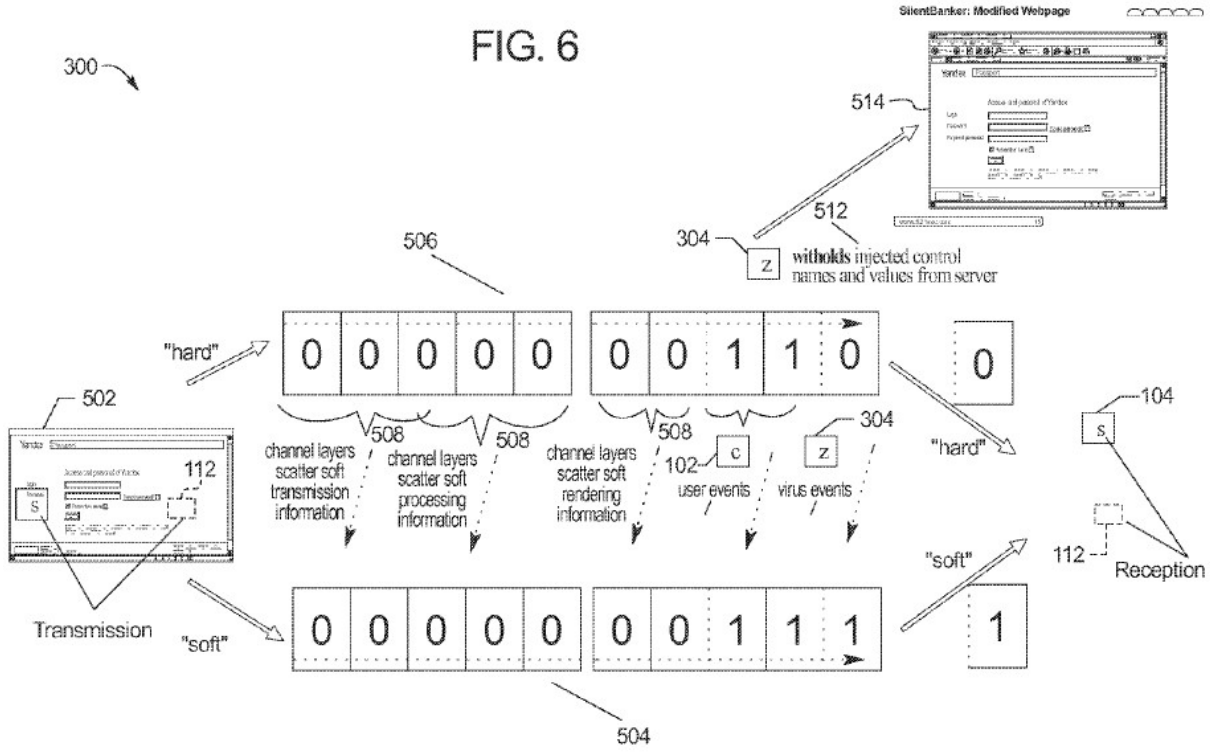
56. The '870 Patent details how the security processor in the communications network creates a prediction for the mouse click on the "submit" button and detects the malicious application by determining that the coordinates of the mouse click do not match the coordinates of the "submit" button made during the prediction. In one example, while the malicious application can remove the response to a security question and create channel noise so that the server is never made aware that no answer to the security question has been provided, the system

claimed in the ’870 Patent can use the security processor to detect the malicious application because the malicious application is not concerned with the mouse click information and accordingly does not alter the soft information.

FIG. 5



’870 Patent at Fig. 5.



'870 Patent at Fig. 6.

57. At least claims 1-2, 4-11, 17-21, 37-39, and 42-43 of the '870 Patent overcome the failings of the prior art, in part, by requiring "providing an indication there is a malicious application affecting communications between the server and the client device, wherein the prediction is further determined based at least in part by at least one of: (a) estimating locations of rendered features and functions as displayed by the client device, (b) estimating locations of rendered page geometry of the features and functions, (c) estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device, (d) estimating a label of the presentation information, (e) estimating a utilization of a codeword set

based on the presentation information and transactional information, and (f) estimating a utilization of a codeword set based on actions taken by at least one of the user and the client device." *Id*. at cl. 1.

58. A person of ordinary skill in the art at the time of the invention would have understood that the focus of the '870 Patent claims is on the specific asserted improvement in computer capabilities and operation (*i.e.*, validating communications in an open architecture system and varying soft information related to the display of hard information) rather than on an economic or other task for which a computer is used in its ordinary capacity.

59. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating locations of rendered features and functions as displayed by the client device" was not, at the time of the invention, conventional, well-understood, or routine.

60. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating locations of rendered page geometry of the features and functions" was not, at the time of the invention, conventional, well-understood, or routine.

61. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device" was not, at the time of the invention, conventional, well-understood, or routine.

62. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a label of the presentation information" was not, at the time of the invention, conventional, well-understood, or routine.

63. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a utilization of a codeword set based on the presentation information and transactional information" was not, at the time of the invention, conventional, well-understood, or routine.

64. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a utilization of a codeword set based on actions taken by at least one of the user and the client

device" was not, at the time of the invention, conventional, well-understood, or routine.

65. A person skilled in the art at the time of the invention would have understood that the '870 Patent claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of computer communications in an open architecture system.

66. These technological improvements provide greater cost savings and efficiencies in preventing malicious software from infecting computers and thereby decreasing fraud and all of the attendant costs to remedying infected computers, ameliorating client account issues, etc.

67. The novel use and arrangement of the specific combinations and steps recited in the claims of the '870 Patent were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

THE '682 PATENT

68. SunStone is the owner by assignment from the inventor, David Ford, of all right, title, and interest in and to United States Patent Number 10,958,682 (the "'682 Patent"), titled "Methods and Apparatus for Varying Soft Information Related to the Display of Hard Information" including the right to sue for all past, present, and future infringement.

69. Exhibit Z is a true and correct copy of the '682 Patent.

70. The ’682 Patent issued from United States Patent Application Serial No. 16/298,537 (the “’537 Application”) filed on March 11, 2019.

71. The ’682 Patent claims priority to United States Patent No. 10,230,759, filed August 31, 2015, which in turn claims priority to United States Patent No. 9,122,870, filed September 20, 2012, which then claims priority to United States Provisional Patent Application Serial No. 61/557,733, filed on November 9, 2011, and United States Provisional Patent Application Serial No. 61/537,380, filed on September. 21, 2011.

72. The United States Patent and Trademark Office published the ’537 Application on February 6, 2020.

73. Since February 6, 2020, all papers in the ’537 Application prosecution file were available to the public.

74. On December 17, 2020, the USPTO allowed claims 2, 6, 8, 11, 13, 16, 19-20, 24-27, 30-31, 33-36, 38-40, 42-44, and 47 of the ’537 Application.

75. On December 18, 2020, SunStone paid the issue fee for the ’537 Application.

76. On February 4, 2021, the USPTO verified the issue fee payment.

77. IBM had knowledge of the ’537 Application at least as early as December 21, 2020.

78. Pursuant to 35 U.S.C. § 154(d), SunStone provided notice of the '537 Application to IBM on December 21, 2020, via its counsel on during a conference call and subsequent email communication.

79. IBM had actual notice of the published patent application at least as early as December 21, 2020.

80. IBM makes, uses, offers for sale, or sells in the United States the invention as claimed in the published patent application.

81. The United States Patent and Trademark Office issued the '682 Patent on March 23, 2021, after a full and fair examination.

82. The '682 Patent is valid and enforceable.

83. The '682 Patent is cited on the face of numerous patents by SunStone's competitors.

84. The '682 Patent describes a method for validating communications in an open architecture system.

85. The '682 Patent describes a method for validating communications in an open architecture system:

> selecting, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device;
>
> selecting, via the processor, presentation information corresponding to the transactional information to transmit from the server to the client

device, the presentation information specifying how the transactional information is to be displayed;

transmitting, via the processor, at least one message including the presentation and transactional information from the server to the client device;

determining, via the processor, a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information specified by the presentation information, and iii) expected response information associated with the transactional information that is expected to be provided by a user of the client device;

receiving, in the processor, the response message from the client device; and

responsive to information in the response message not matching the prediction, providing, via the processor, an indication there is a malicious application affecting communications between the server and the client device,

wherein the prediction is further determined by the processor based at least in part by estimating at least one location of at least one rendered feature or function as displayed by the client device,

wherein the presentation information includes at least one of protocol information, formatting information, positional information, rendering information, style information, transmission encoding information, information describing how different layers of a style sheet are to be rendered by the client device, or information changing a definition of a function in a code library at the client device, and

wherein the transactional information includes at least one of text, data, pictorial information, image information, information requested by the server to perform a service for the client device, authentication information, refinement information on a type of service requested by the client device, financial information, or data management information.

’682 Patent, Claim 1.

86. The ’682 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination by the United States Patent and Trademark Office.

87. The ’682 Patent is directed to a novel apparatus and method for validating communications between servers and client devices. As described by the specification, communications between servers and client devices were prone to problems specific to computer communications:

> Using malicious noise, viruses and other types of malicious applications are able to direct a client device (*e.g.*, a receiver) to perform actions that a communicatively coupled server (*e.g.*, a sender) did not originally intend. Additionally, the viruses and malicious applications are able to direct a server to perform actions that communicatively coupled client devices did not originally intend. Conventional virus detection algorithms often fail to detect the malicious nature of the noise because these algorithms are configured to detect the presence of the noise’s source rather than the noise itself. The noise generation algorithm (*e.g.*, the code of the malicious application) is relatively easily disguised and able to assume a wide variety of formats. There is accordingly a need to validate communications between servers and client devices in the presence of malicious noise.

’682 Patent at 2:37-51.

88. An example embodiment of the ’682 Patent includes a method of selecting transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device, selecting presentation information corresponding to the transactional information to transmit

from the server to the client device, transmitting at least one message including the presentation and transactional information from the server to the client device, determining a prediction as to how the client device will render the transactional information based on the presentation information, receiving a response message from the client, and responsive to information in the response message not matching the prediction, providing an indication there is a malicious application affecting communications between the server and the client device.

89. The '682 Patent describes a network communication system that includes one or more client devices, application servers, and database servers connected to one or more databases. Each of the client devices may communicate with one another on the network, such as for example, the Internet or a local area network. The application servers may provide services accessible to the client devices while the database servers provide a framework for the client devices to access data stored in the databases. The application servers can provide, for example, banking services, government services, etc. After selecting which soft and hard information to send to the client device, the security processor makes a prediction, such as, the location of a "Submit" icon on a fully rendered webpage that is part of a banking website provide by the application server. The security processor then monitors responses by the client device to identify coordinates of a mouse click of the "Submit" icon to determine if a malicious application is affecting

communications if the prediction does not match the reported coordinates of the mouse click. The security processor would then attempt to prevent the malicious application from further communications with the affected client device.

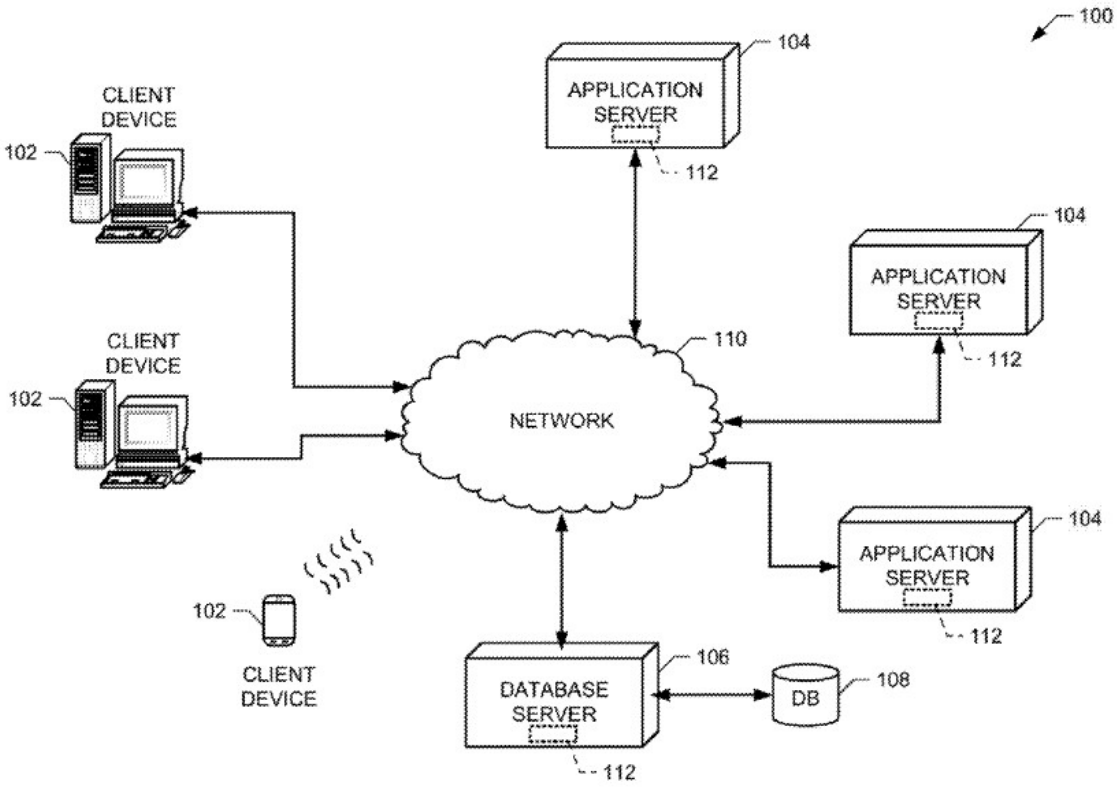


FIG. 1

'682 Patent at Fig. 1.

90. The client devices, application servers, and database servers described above would include computing devices with microprocessors, memory, an interface circuit (which may be implemented using any suitable interface standard, such as, for example, an Ethernet interface and/or a Universal Serial Bus (USB) interface), and storage devices such as a hard drive.

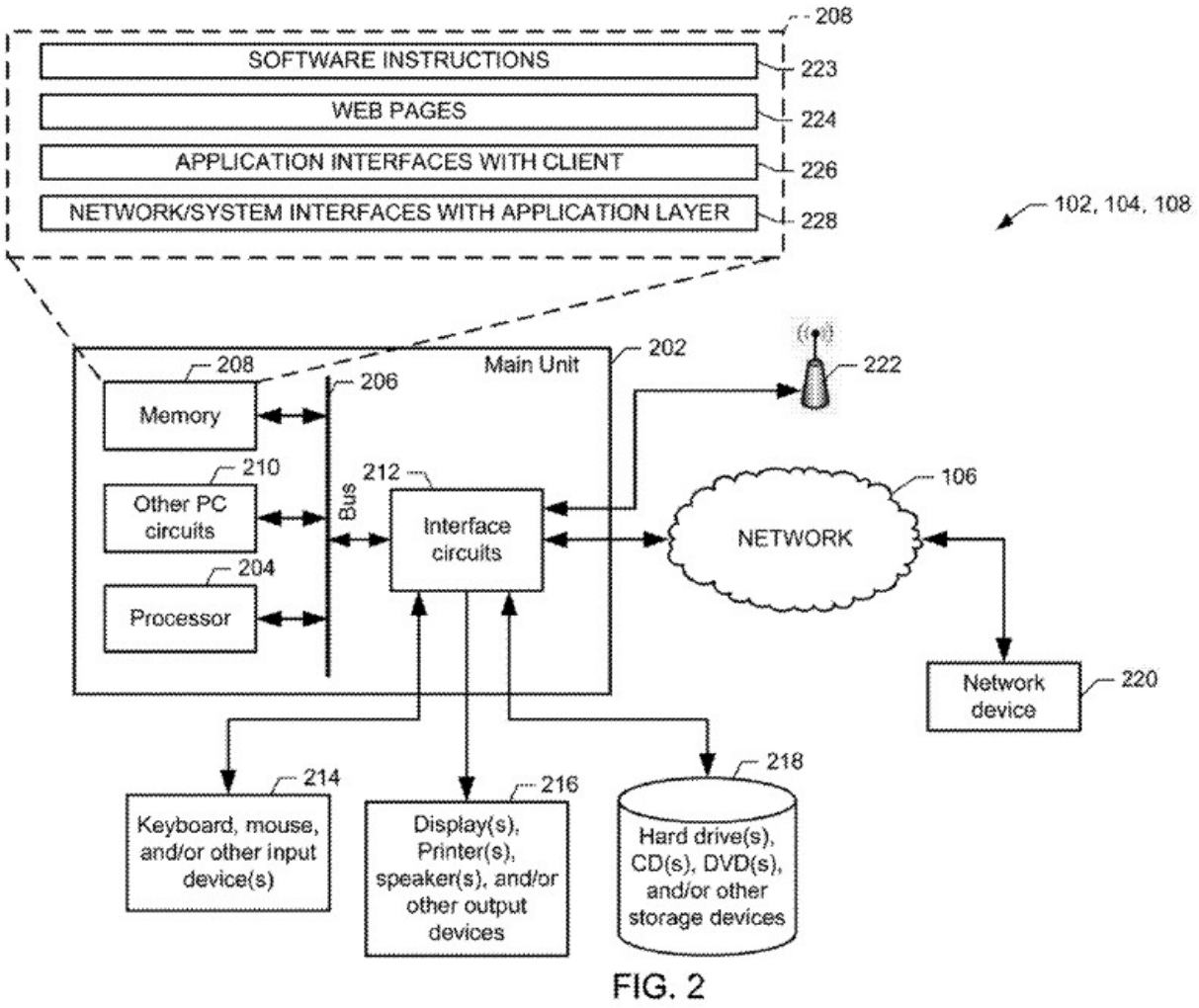


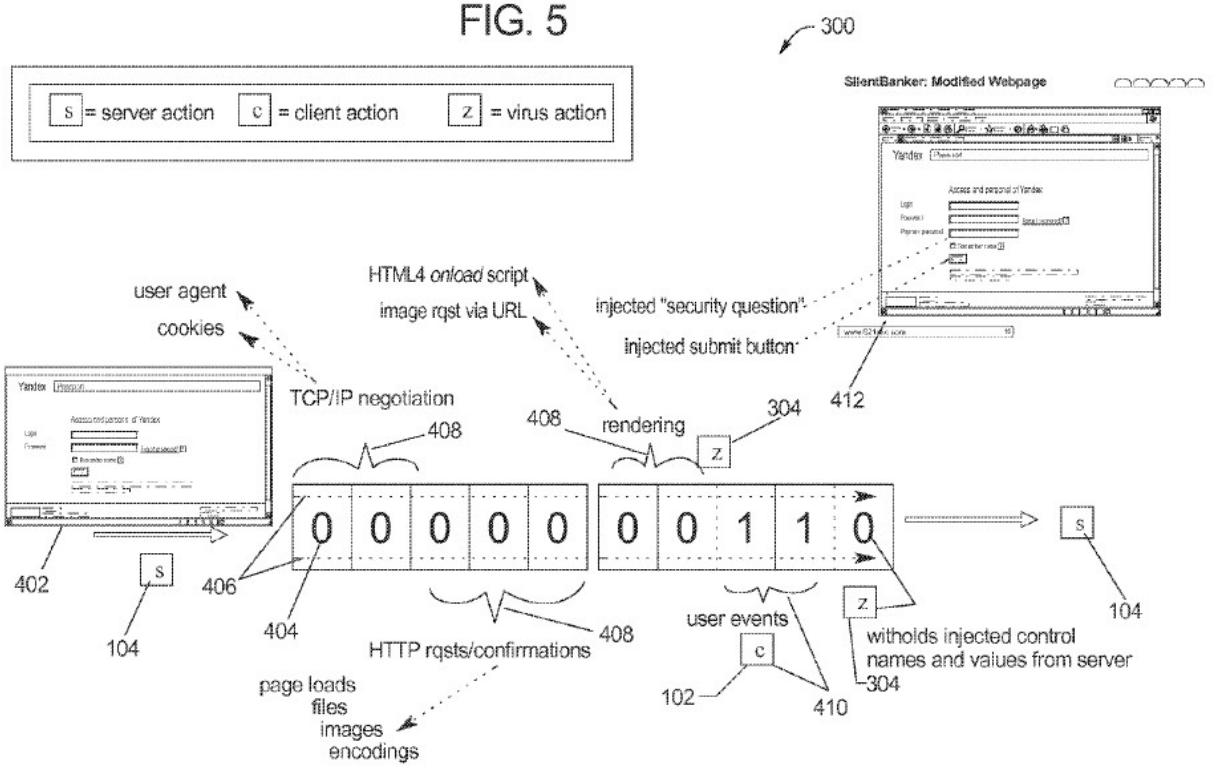
FIG. 2

'682 Patent at Fig. 2.

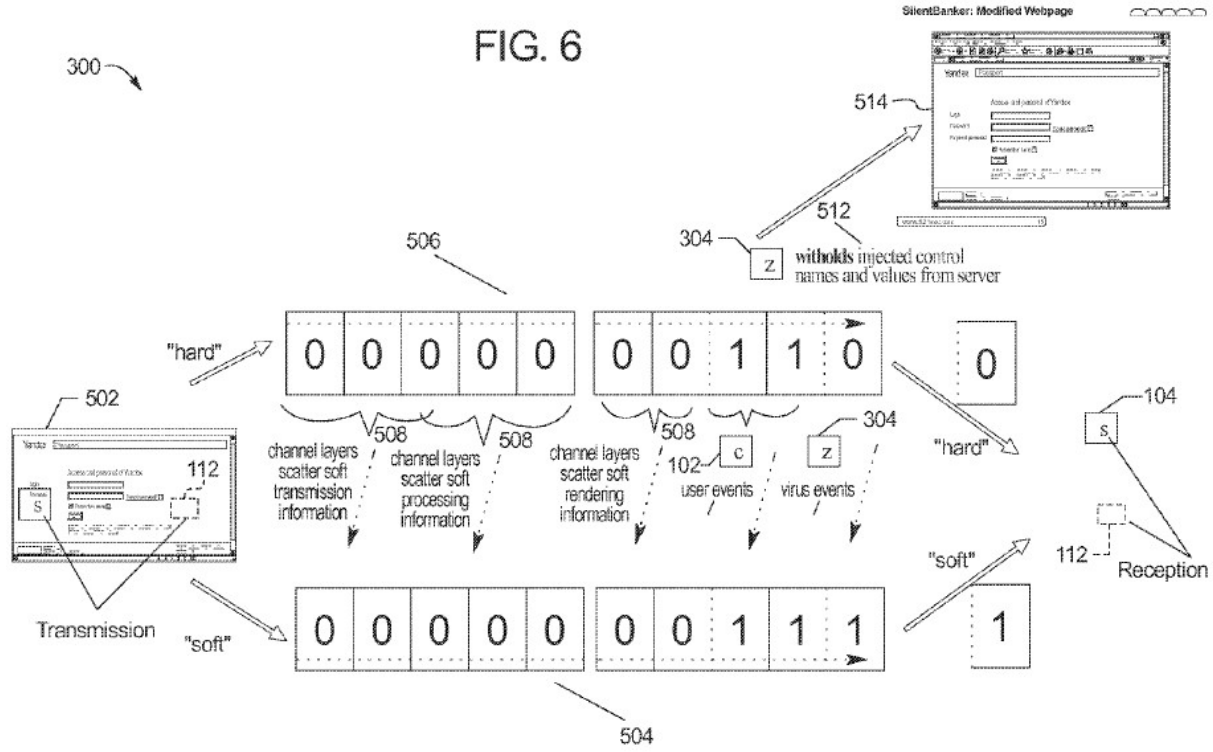
91. The '682 Patent details how the security processor in the communications network creates a prediction for the mouse click on the "submit" button and detects the malicious application by determining that the coordinates of the mouse click do not match the coordinates of the "submit" button made during the prediction. In one example, while the malicious application can remove the response to a security question and create channel noise so that the server is never made aware that no answer to the security question has been provided, the system

claimed in the ’682 Patent can use the security processor to detect the malicious application because the malicious application is not concerned with the mouse click information and accordingly does not alter the soft information.

FIG. 5



’682 Patent at Fig. 5.



'682 Patent at Fig. 6.

92. At least claims 1-11 and 21-29 of the '682 Patent overcome the failings of the prior art, in part, by requiring "providing, via the processor, an indication there is a malicious application affecting communications between the server and the client device, wherein the prediction is further determined by the processor based at least in part by estimating at least one location of at least one rendered feature or function as displayed by the client device." *Id*. at cl. 1.

93. A person of ordinary skill in the art at the time of the invention would have understood that the focus of the '682 Patent claims is on the specific asserted improvement in computer capabilities and operation (*i.e.*, validating

communications in an open architecture system and varying soft information related to the display of hard information) rather than on an economic or other task for which a computer is used in its ordinary capacity.

94. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating locations of rendered features and functions as displayed by the client device" was not, at the time of the invention, conventional, well-understood, or routine.

95. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating locations of rendered page geometry of the features and functions" was not, at the time of the invention, conventional, well-understood, or routine.

96. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device" was not, at the time of the invention, conventional, well-understood, or routine.

97. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a label of the presentation information" was not, at the time of the invention, conventional, well-understood, or routine.

98. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a utilization of a codeword set based on the presentation information and transactional information" was not, at the time of the invention, conventional, well-understood, or routine.

99. A person skilled in the art at the time of the invention would have understood that the step of predicting whether a malicious application was affecting communications between the server and client device by "estimating a utilization of a codeword set based on actions taken by at least one of the user and the client device" was not, at the time of the invention, conventional, well-understood, or routine.

100. A person skilled in the art at the time of the invention would have understood that the '682 Patent claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of computer communications in an open architecture system.

101. These technological improvements provide greater cost savings and efficiencies in preventing malicious software from infecting computers and thereby decreasing fraud and all of the attendant costs to remedying infected computers, ameliorating client account issues, etc.

102. The novel use and arrangement of the specific combinations and steps recited in the claims of the '682 Patent were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

IBM TRUSTEER

103. Trusteer, Inc. was founded in Israel in 2006 by Mickey Boodaei and Rakesh K. Loonkar. IBM acquired Trusteer in 2013. Trusteer's products and services are part of IBM Security Trusteer fraud detection.

104. Trusteer's products aim to block online threats from malware and phishing attacks, and to support regulatory compliance requirements. Trusteer's products aim to prevent incidents at the point of attack while investigating their source to mitigate future attacks. In addition, Trusteer's products allow organizations to receive immediate alerts, and to report or flag to the organization whenever a new threat is launched against them or their customers. *See* Ex. B, Amanda Ciccatelli, MobilityTechzone, *Protect Your Enterprise from Devastating Advanced Malware* (Feb. 13, 2013), *available at*

http://www.mobilitytechzone.com/topics/4g-wirelessevolution/articles/2013/02/13/326747-protect-enterprise-from-devastating-advanced-malware.htm.

105. Trusteer's first commercial product was Trusteer Rapport. Trusteer Rapport is security software advertised as an additional layer of security to anti-virus software. It is designed to protect confidential data, such as account credentials, from being stolen by malicious software (malware) and via phishing, *i.e.*, the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. To achieve this goal, the software includes anti-phishing measures to protect against misdirection and attempts to prevent malicious screen scraping; it attempts to protect users against the following forms of attacks: man-in-the-browser, man-in-the-middle, session hijacking and screen capturing. *See* Ex. C, DNSstuff, *DNSstuff.com offers Trusteer Rapport product to help users boost their defenses against online fraud* (Mar. 19, 2009), *available at* https://web.archive.org/web/20150717170925/www.dnsstuff.com/?Itemid=5&id=134&option=com_content&task=view.

106. Trusteer Rapport is still utilized today. *See* Ex. D, IBM, *IBM Security Trusteer Rapport*, *available at* https://www.ibm.com/products/phishing-and-malware-protection.

107. Trusteer Rapport requires the user to download and install software. On installation, Rapport also tries to remove existing financial malware from end-user machines and to prevent future infection. The Trusteer Rapport client is available for multiple platforms in the form of a browser extension. Rapport is supported by Google Chrome, Microsoft Edge, Mozilla Firefox, and Microsoft Internet Explorer on devices running Windows 7 and later. Rapport is also supported by Google Chrome, Mozilla Firefox, and Apple Safari on devices running macOS 10.12 (Sierra) and later.

108. End users have reported problems with Rapport, slow PCs due to high CPU and RAM utilization, incompatibility with various security/antivirus products and difficulty in removing the software. *See* Ex. E, Davey Winder, *Is HSBC's security software more trouble than it's worth?* (Jul. 20, 2010), *available at* https://web.archive.org/web/20100722110757/http://www.pcpro.co.uk/realworld/359617/is-hsbcs-security-software-more-trouble-than-its-worth.

109. The consumer organization *Which?* found that many members had problems due to running Trusteer Rapport and advised against using it. They found that it could conflict with other security software, and slow or crash the Web browser. *Which?* emphasizes that it is the bank's responsibility, not Rapport's, to protect customers' online banking, adding that online banking can be perfectly safe without Trusteer Rapport; its only benefit would be detecting a phishing site

masquerading as the bank—"but plenty of other tools, including most modern browsers, can do this anyway." They clarify that the software is legitimate and respectable, but "don't feel the claims on Rapport's website add up." *See* Ex. F, Which?, *Should you use Trusteer Rapport? – Which Computing Helpdesk* (Aug. 21, 2010), *available at* https://computing.which.co.uk/hc/en-gb/articles/115005579745-Should-you-use-Trusteer-Rapport-.

110. In a presentation given at 44con in September 2011, bypassing Trusteer Rapport's keylogger protection was shown to be relatively trivial. *See* Ex. G, Neil Kettle, *44Con and Trusteer Rapport, Digit Security Blog* (Sept. 7, 2011), *available at* http://www.digit-security.com/blog/?p=47. Shortly thereafter Trusteer confirmed that the flaw was corrected and said that even if a hacker were able to use the flaw to disable anti-keylogging functions in Rapport, other secondary security protection technologies would still be in play. *See* Ex. H, John Leyden, *Trusteer rebuffs bank security bypass claims*. (Oct. 11, 2011), *available at* https://www.theregister.co.uk/2011/10/11/trusteer_rapport_security_bypass/.

111. The Trusteer Rapport software is incompatible with Windows tool Driver Verifier and may cause the user to encounter a Blue Screen and system crash. Ex. I, Trusteer Support Website: Driver Verifier, *available at* https://web.archive.org/web/20131103091234/http://www.trusteer.com/support/driver-verifier.

112. Some banks which had offered the software discontinued offering it. For instance, NatWest and Royal Bank of Scotland withdrew use in January 2019, stating that "The security and fraud prevention technologies we now use provide you a higher and far broader level of protection." *See* Ex. J, NatWest, *Important Information for IBM Rapport Users*, *available at* https://personal.natwest.com/personal/fraud-and-security/rapport.html; Ex. K, RBS, *Important Information for IBM Rapport Users*, *available at* https://personal.rbs.co.uk/personal/fraud-and-security/rapport.html.

113. In October 2011, Trusteer introduced PinPoint Cloud Service. PinPoint Cloud service examines internet traffic for signs the user's desktop is infected with trojans such as SpyEye and Zeus that can steal funds or data. *See* Ex. L, *eWeek, Trusteer Pinpoint Cloud Service Protects Against Malware Fraud* (Mar. 17, 2011), *available at* https://www.eweek.com/security/trusteer-pinpoint-cloud-service-protects-against-malware-fraud.

114. Trusteer's 2013 revenue was approximately $100 million. Trusteer's 2014 revenue was approximately $140 million. *See* Ex. M, Globes, *Trusteer prevents hackers attacking bank accounts* (Nov.18, 2012), *available at* https://en.globes.co.il/en/article-1000799100; Ex. N, *Trusteer Acquired By IBM For An Estimated $800M* (Aug 15, 2013), *available at* http://nocamels.com/2013/08/trusteer-acquired-by-ibm-for-an-estimated-800m/.

115. Trusteer more than doubled its customer base between 2013 to 2015. *See* Ex. O, *IBM Buys Israel/US Cybersecurity Specialist Trusteer For $800M-$1B* (Aug. 15, 2013), *available at* https://techcrunch.com/2013/08/15/ibm-buys-israelus-cybersecurity-specialist-trusteer-for-few-hundred-million-dollars/.

116. IBM purchased Trusteer in 2013 for between $800 million and $1 billion and continued development of Trusteer's products and services. *See* Ex. P, *Trusteer Acquired By IBM For An Estimated $800M* (Aug 15, 2013), *available at* http://nocamels.com/2013/08/trusteer-acquired-by-ibm-for-an-estimated-800m/.

117. On October 27, 2016, IBM introduced Trusteer Pinpoint Detect, which incorporates behavior biometrics and cognitive processing. *See* Ex. Q, IBM, *IBM Security Adds Cognitive Behavioral Biometrics to Help Protect Banking Customers from Cybercrime, New Trusteer Technology to Help Prevent Bank Fraud* (Oct. 27, 2016), *available at* https://newsroom.ibm.com/2016-10-27-IBM-Security-Adds-Cognitive-Behavioral-Biometrics-to-Help-Protect-Banking-Customers-from-Cybercrime.

118. According to IBM, Trusteer Pinpoint Detect works transparently, without the need for downloading executable files or plug-ins to the end user's computer. For web applications, Pinpoint uses code embedded into the webpage. For Trusteer Pinpoint Detect mobile applications, the organization's app uses the IBM

Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

119. IBM ties the sales of Trusteer Pinpoint Detect to other products and services offerings. For example, according to IBM's services description, "[s]ubscription to IBM Trusteer Detect Standard or IBM Trusteer Pinpoint Detect Premium or IBM Security Pinpoint Detect Standard with access management integration or IBM Security Detect Premium with access management integration is a prerequisite to" receiving "associated additional Cloud Services." Ex. S at 5, *IBM Service Description*.

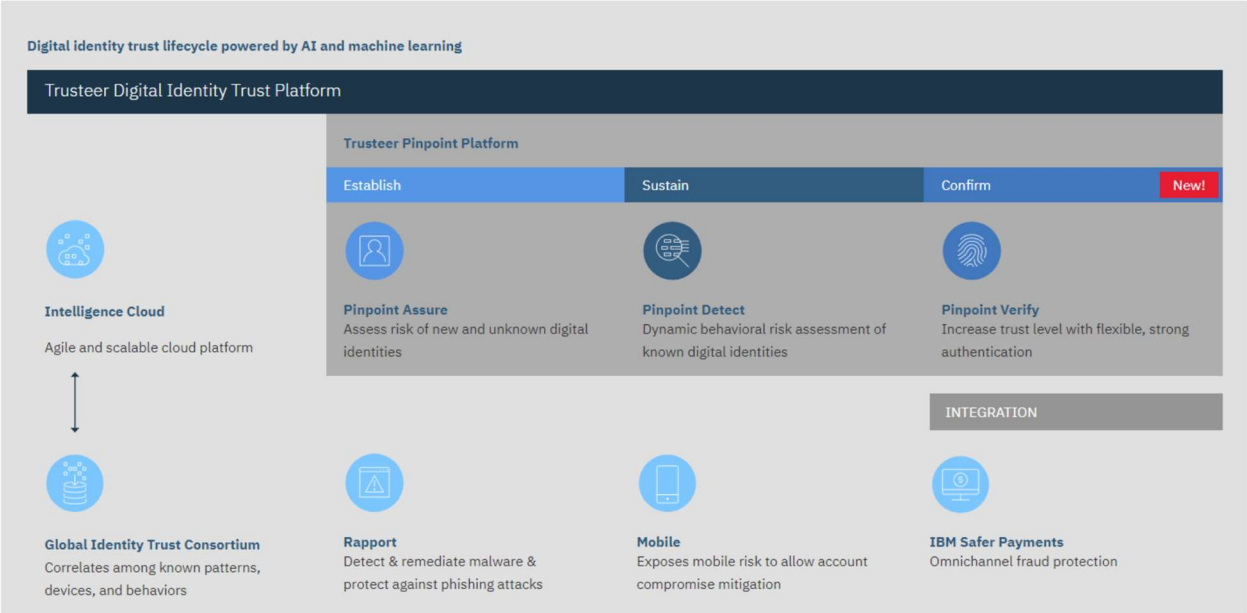
120. IBM revenue growth for the security sector averaged approximately 15 to 20 percent in the years 2015 through 2018. *See* Ex. T, *IBM earnings: Security is growing fast, but is it enough money to matter?* (Jul. 18, 2020), *available at* https://www.marketwatch.com/story/ibm-earnings-security-is-growing-fast-but-is-it-enough-money-to-matter-2018-07-13.

121. Upon information and belief, IBM's estimated average incremental profit margin for 2017 through 2019 was approximately 20 to 22 percent. *See* Ex. U, Finbox.com, IBM, *available at* https://finbox.com/NYSE:IBM/models. Upon information and belief, IBM has gross margins of approximately 46 to 48 percent, and operating margins of approximately 14 to 15 percent. *Id*.

THE ACCUSED PRODUCTS

122. According to IBM, the IBM Trusteer platform combines many of IBM's strengths to give continuous digital identity assurance and context-based authentication, regardless of the industry such as: AI and machine learning infused with security intelligence service, scalable agile cloud platform powered by a global network of risk expertise, and end-to-end strategy for building digital identity trust across the omnichannel journey. Ex. V, *IBM Digital eBook*, *available at* https://www.ibm.com/security/resources/trusteer/know-the-real-me/.

123. According to IBM, Trusteer products aim to prevent incidents at the point of attack while investigating their source to mitigate future attacks. In addition, IBM's Trusteer products allow organizations to receive immediate alerts, and to report or flag to the organization whenever a new threat is launched against them or their customers.

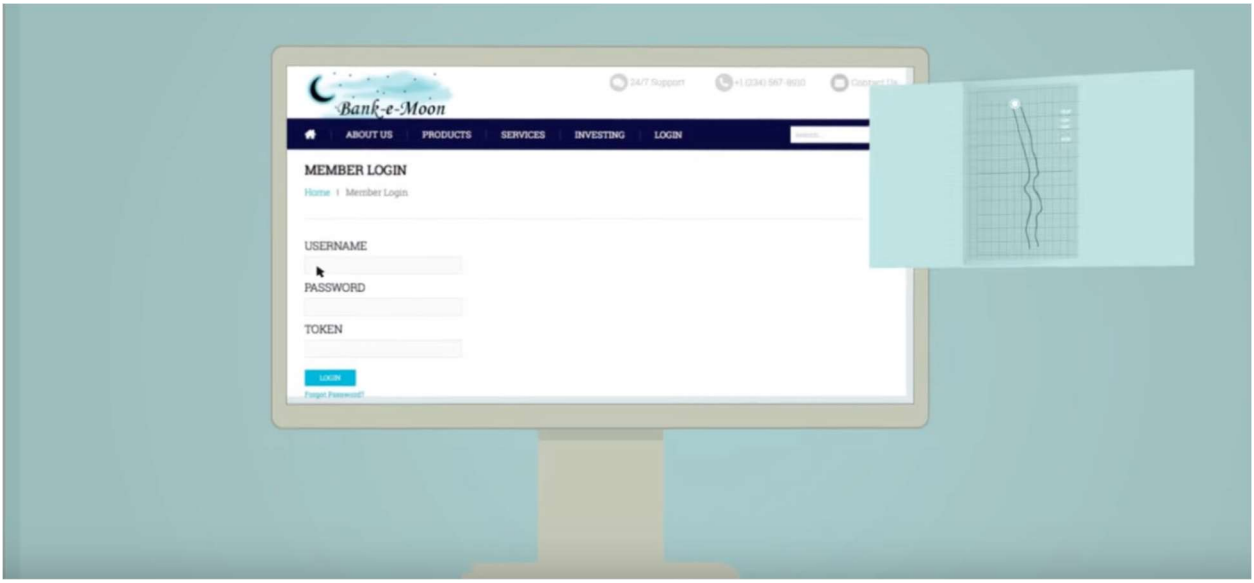


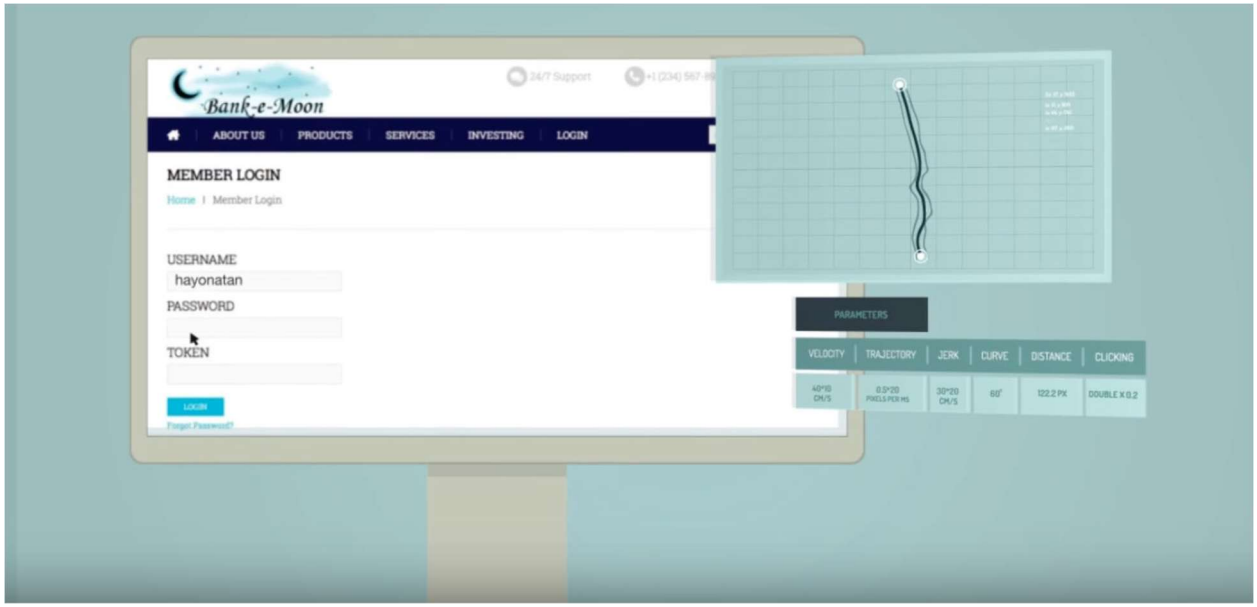
124. There are a wide variety of IBM Trusteer products that utilize this technology including, at least, Trusteer Pinpoint Detect and Trusteer Mobile. The Trusteer Pinpoint Detect detection software module may be a snippet of code (*e.g.*, JavaScript) that is integrated into the legitimate transaction page of the bank. This code is adapted to detect exception-causing activity conditions with the web page during a session. Such conditions include automatic filling of the required fields in a transaction form and browsing to another remote location during a session to retrieve details of a mule account, *i.e.*, an account created by criminals using stolen or synthetic identities. Other parameters can be used by the detection module to determine whether an Iframe (an inline frame (Iframe) is used to embed another document within the current HTML document) is a part of the bank's original webpage or if this Iframe has been created by the malware.

125. Once such an exception-causing activity condition is detected, the detection module can mark the transaction as a fraud transaction, block the transaction, report the exception to the bank and/or to other authorities, or extract the details of the mule account from the transaction form before the "submit" button is activated.

126. A demonstration of the Trusteer Pinpoint Detect technology can be found at https://www.youtube.com/watch?v=kemFd5t2nD4.

127. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect software utilizes predictions based on one or more of estimating locations of rendered features and functions as displayed by the client device, estimating locations of rendered page geometry of the features and functions, estimating a label of the presentation information, and estimating a utilization of a codeword set based on the presentation information and transactional information.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

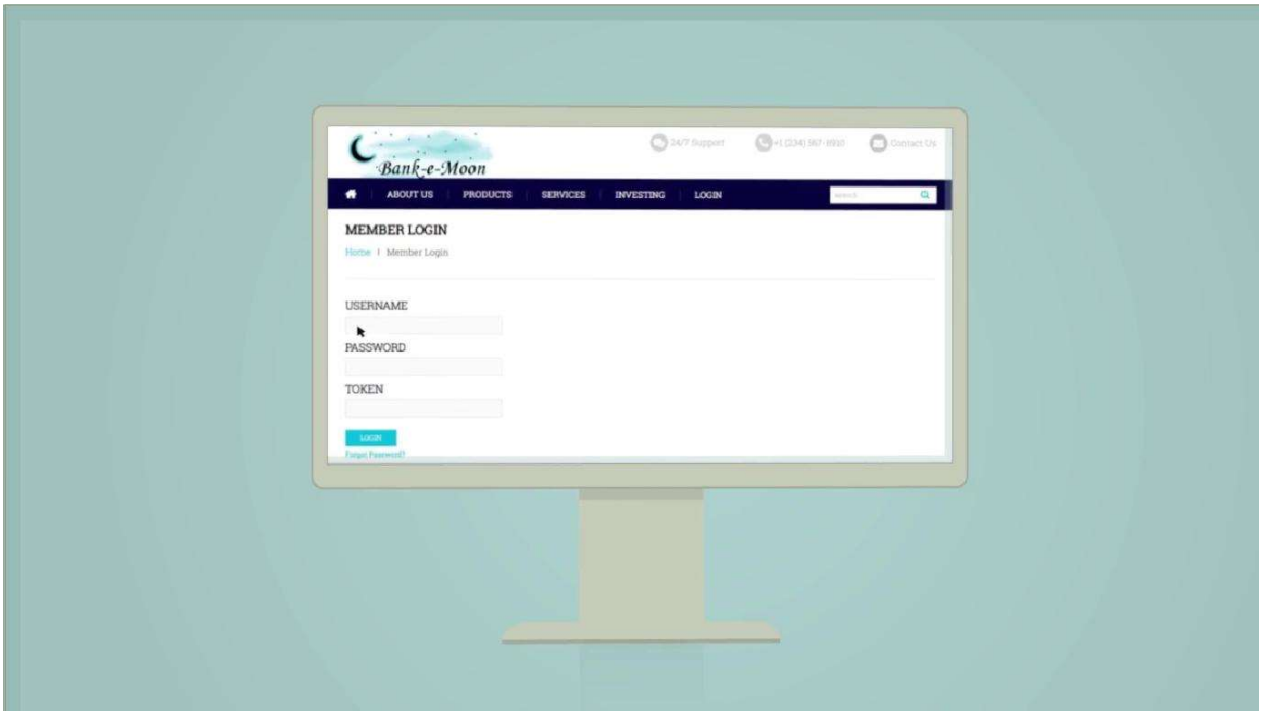
128. According to IBM, Trusteer Pinpoint Detect is deployed as a software as a service (SaaS) solution. It is designed to help organizations quickly and transparently establish digital identity trust. This can allow them to create a more seamless customer experience, without compromising on security. Trusteer Pinpoint Detect uses artificial intelligence and machine learning to help protect digital channels against account takeover and fraudulent transactions and can help detect end-user devices infected with high-risk malware. Trusteer Pinpoint Detect is a cloud-based solution that provides risk assessment for online identities to help differentiate between malicious users and true customers. *See* Ex. W, IBM, *Trusteer*

Pinpoint Detect Overview, *available at* https://www.ibm.com/us-en/marketplace/trusteer-pinpoint-detect.

129. Trusteer Pinpoint Detect is available for mobile solutions, Trusteer Mobile, which helps detect real-time device and session risks. According to IBM, Trusteer Pinpoint Detect helps maintain the integrity of the application in which it has been enabled by leveraging advanced analytics and real-time device risk detection. Trusteer Mobile assesses the device to determine if it is compromised such as by malware, remote access trojans, jailbroken/rooted detection, overlay attack evidence and SMS stealing apps. Additional cross-channel indicators are continuously processed leveraging advanced technologies such as behavioral anomalies, navigation discrepancies and phishing compromise. *See* Ex. X, IBM, *Mobile SDK*, *available at* https://www.ibm.com/us-en/marketplace/trusteer-mobile-sdk. Trusteer Mobile uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

130. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in Trusteer Pinpoint Detect, a server, such as, for example, the Bank-e-Moon server illustrated in the Behavioral Biometrics Demo Video, receives a request for the member login web page from the Client device. In response to that request, the server has selected the transactional information (hard information) to request from

the client. In the Bank-e-Moon demo provided by IBM, the server is requesting a "USERNAME," "PASSWORD," and "TOKEN."



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

131. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect next provides for selecting presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. For example, as shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the server has received a request for the

member login web page from the Client device. The presentation information was selected before sending the code to the client device.

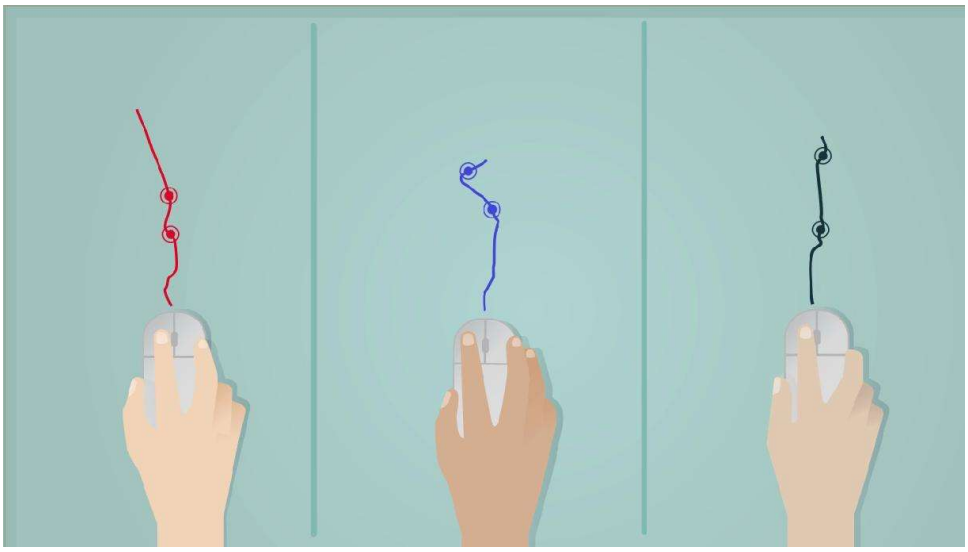
132. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect selects presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. Trusteer Pinpoint Detect accomplishes this by attaching mousemove event listener to the rendered page for the purposes of asking for clientX, clientY (*i.e.*, the X, Y coordinates of the mouse click). Trusteer Pinpoint Detect attaches mousedown mouseup click event listeners on the selected transactional fields – username and password. The event listener functions are re-polymorphed each session.

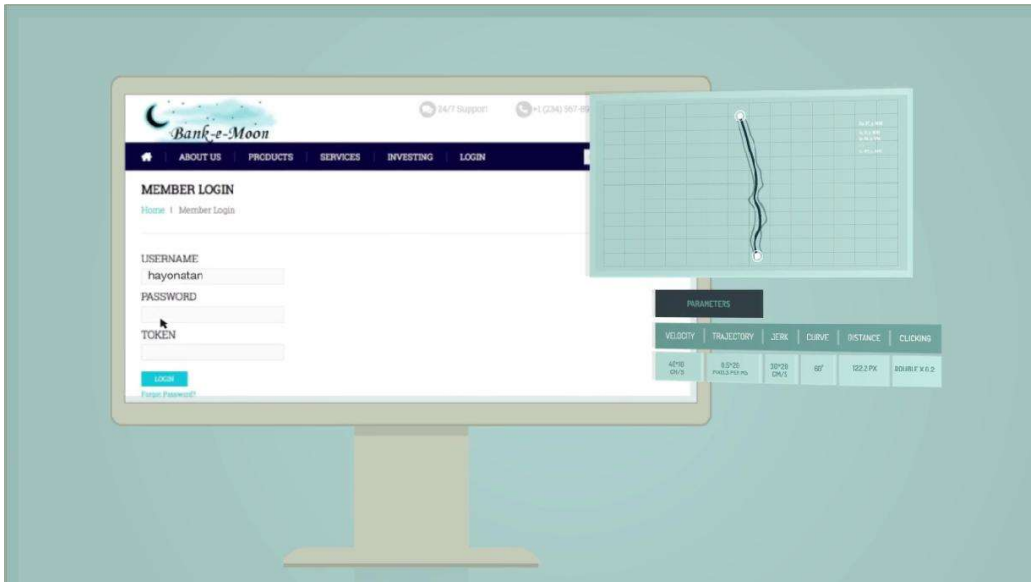
133. According to IBM, Trusteer Pinpoint Detect inputs JavaScript into the client's web browser. According to IBM, Trusteer Pinpoint Detect works transparently, without the need for downloading executable files or plug-ins to the end user's computer. For web applications, Trusteer Pinpoint Detect uses code embedded into the webpage. For mobile applications, the organization's app uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

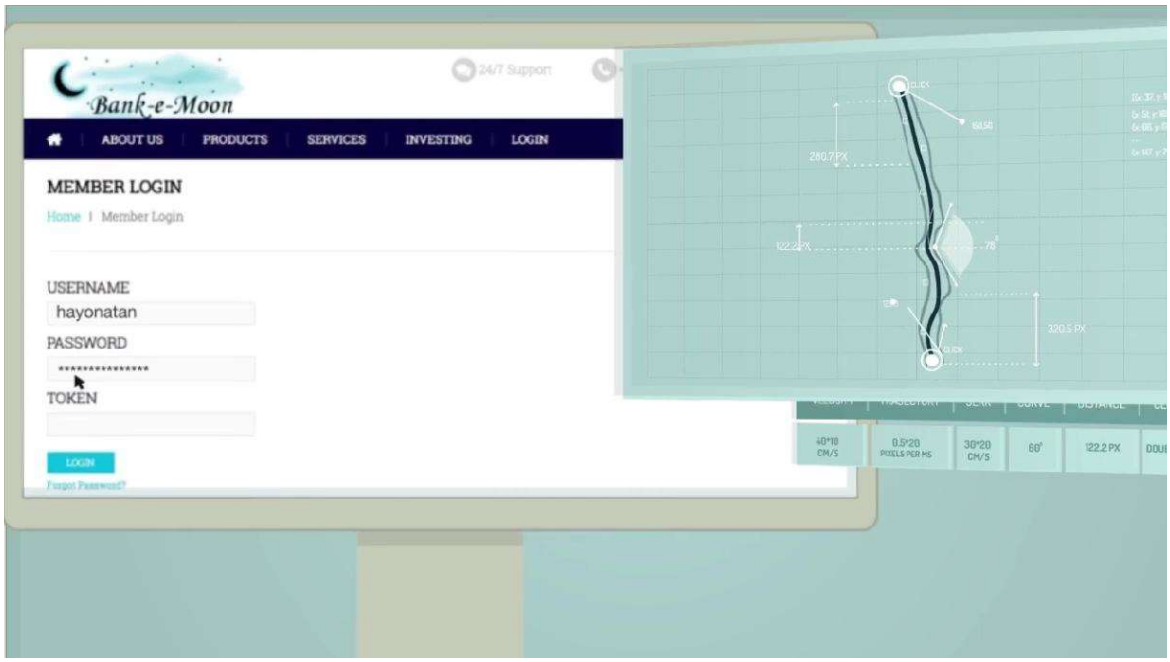
134. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect transmits at least one message including the presentation and transactional information from the server to the client device. This is illustrated by the displayed rendering of the information on the client's device.

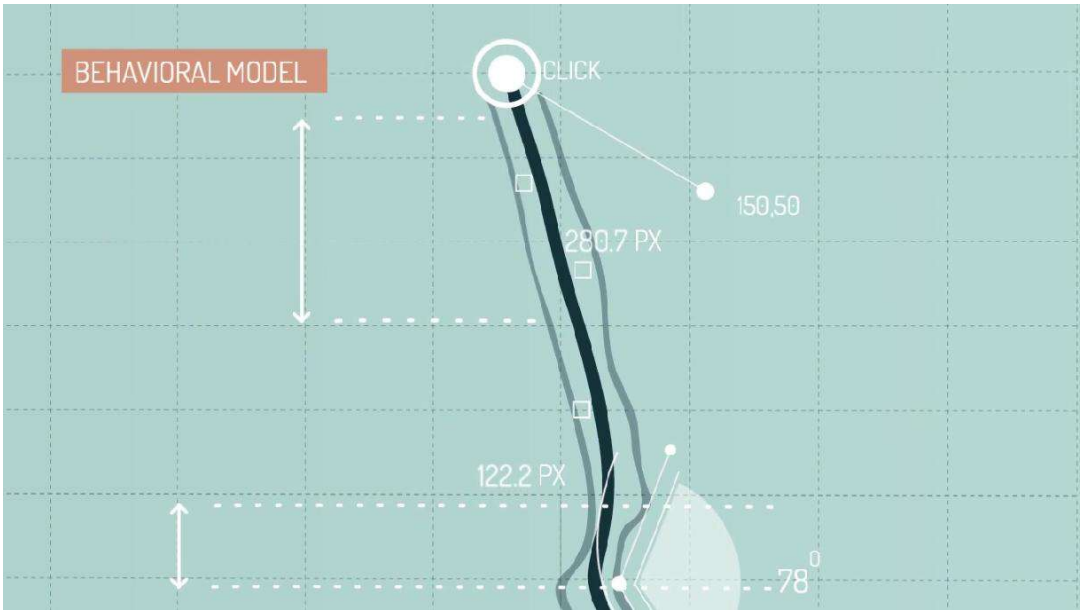
135. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect determines a prediction of a response message from a client device based on (i) the selected transactional information; (ii) how the client device is configured to render the transactional information specified by the presentation information, and (iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device. For example, Trusteer Pinpoint Detect tracks (in the response message) the mouse movements of the client mouse to determine a unique biometric signature, partly based on the starting and ending locations of the mouse. The predicted response signature for the client (stored in Trusteer Pinpoint Detect memory) is compared to the actual response signature (message from client). Trusteer Pinpoint Detect builds a behavioral biometric model that it expects to see for the client to be authenticated partly based on the rendered locations of the transactional (hard) information. The predicted response message for Trusteer Pinpoint Detect would include entering the client's correct username, mouse click order, mouse locations, number of clicks, and path shape parameters, followed by entering the client's

correct password. The measured path shape parameters include velocity, trajectory, jerk, curvature, and distance.









See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

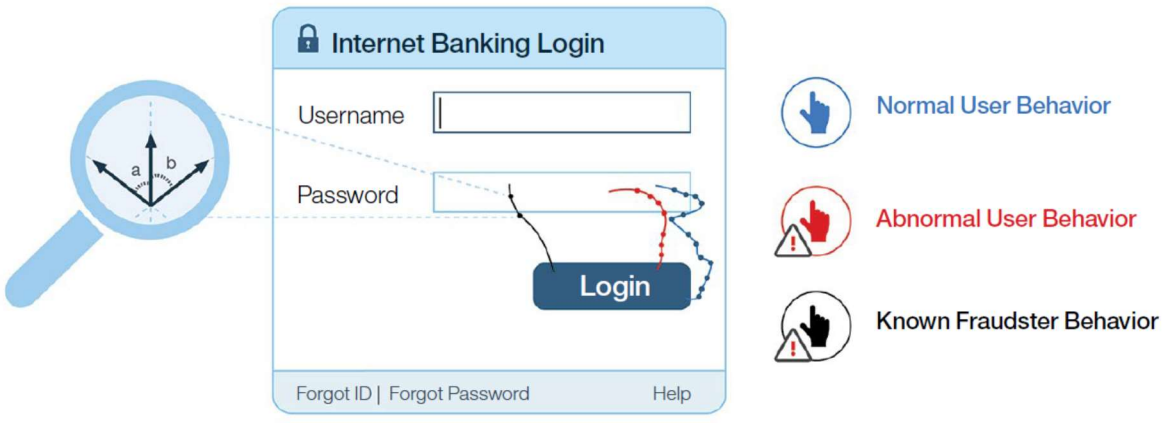
136. IBM accurately describes Trusteer Pinpoint Detect as follows:

IBM Security Trusteer Pinpoint™ Detect now incorporates behavioral biometric capabilities to provide dynamic, context-aware identity analytics that helps improve detection while preserving the user experience.

Built in conjunction with IBM Research labs, the solution's behavioral biometric capability uses machine learning to create a model based on patterns of mouse movements—from login through the entire application flow.

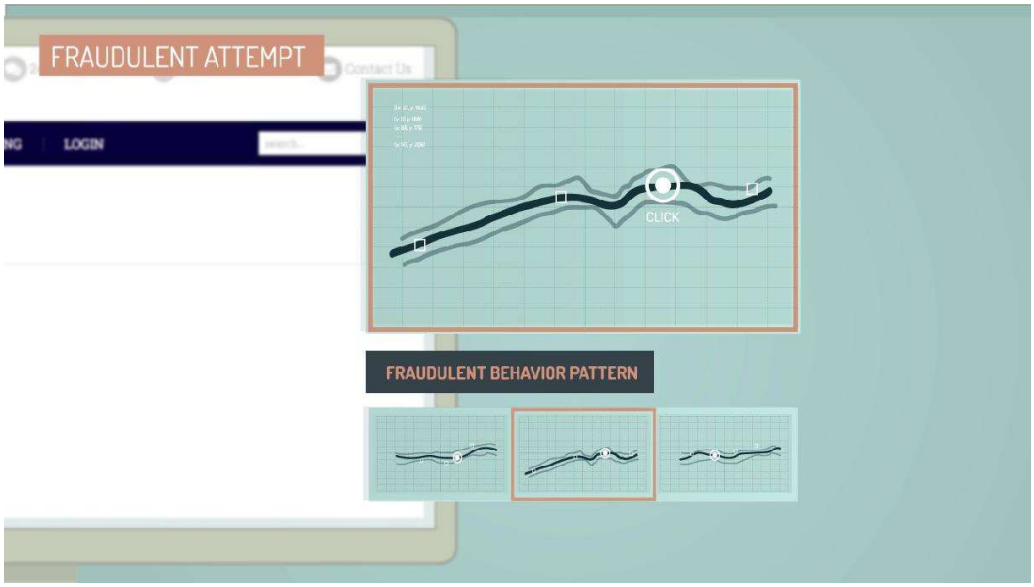
What angle does a user's mouse approach the login box? What direction does the user typically move the mouse? Mouse trajectory, velocity, curvature, jerk, and more are all analyzed.

The platform understands these subtle mouse movements in context and meaning, at astonishing speeds and volumes. It continuously and seamlessly learns user behavior across hundreds of millions of sessions and analyzes current online activity to detect unusual behavior across different devices, even comparing it against observed behavior of known fraudsters for even stronger evidence. If either abnormal user behavior or known fraudster behavior is detected by the platform's sophisticated algorithms, Trusteer Pinpoint Detect provides access management systems and security analysts with a recommended action in real time along with the detailed reasoning and session details so an action can be taken.



Ex. Y, IBM Security, *Thought Leadership White Paper, Shifting the balance of power with cognitive fraud detection*.

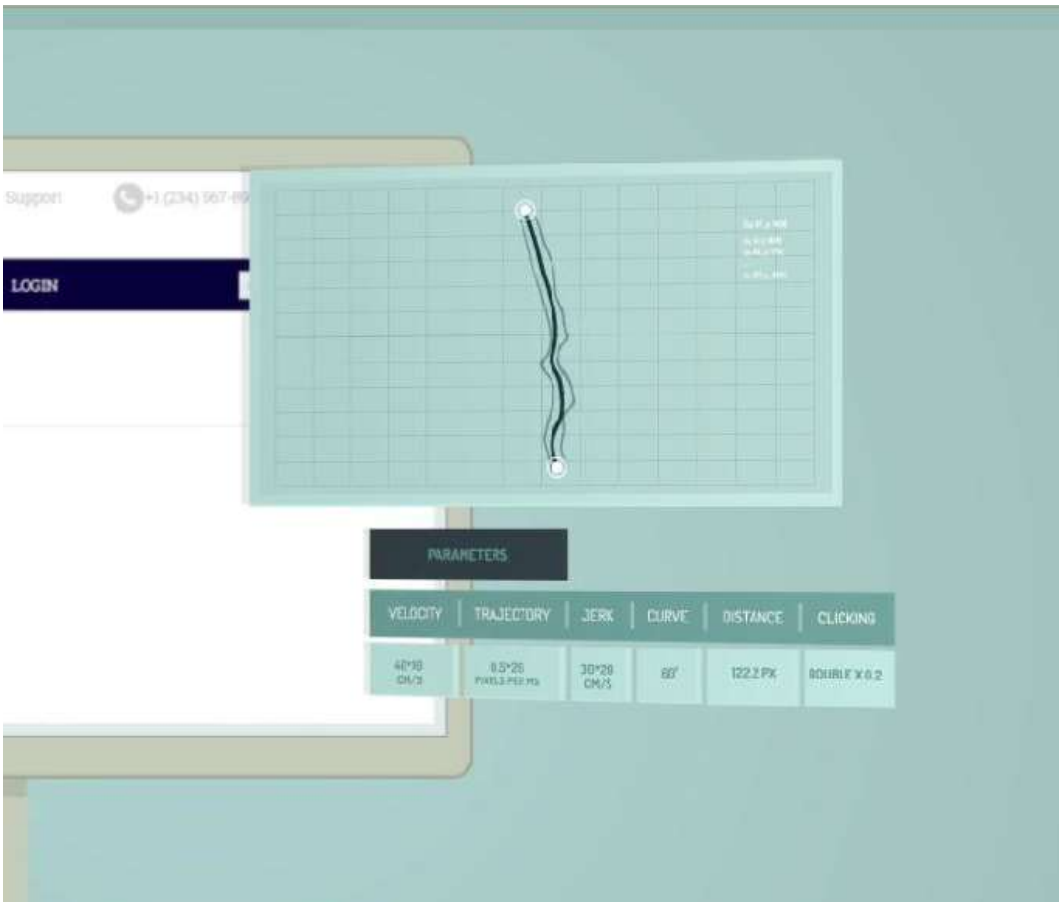
137. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect receives the response message from the client device; and responsive to the information in the response message not matching the prediction, provides an indication there is a malicious application affecting communications between the server and the client device. Trusteer Pinpoint Detect compares the client's mouse path and click locations (based on rendered and displayed transaction information) contained in the response message to the prediction. If there is a match, then the client is authenticated. If it does not match, or matches a known fraudulent behavior pattern, a fraudulent attempt is indicated.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

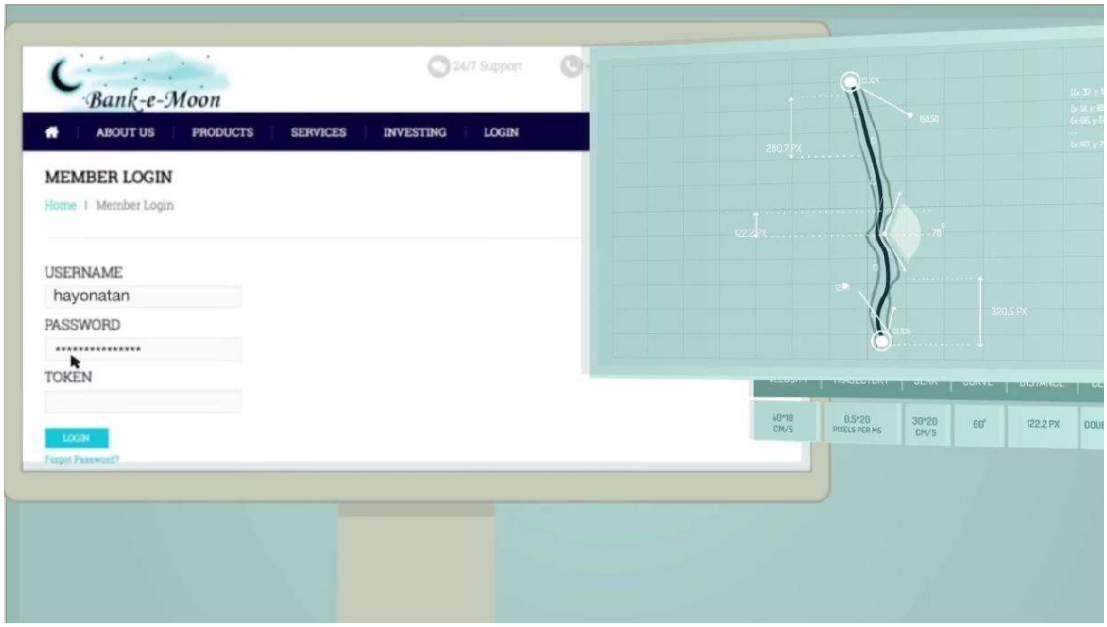
138. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates locations of rendered features and functions as

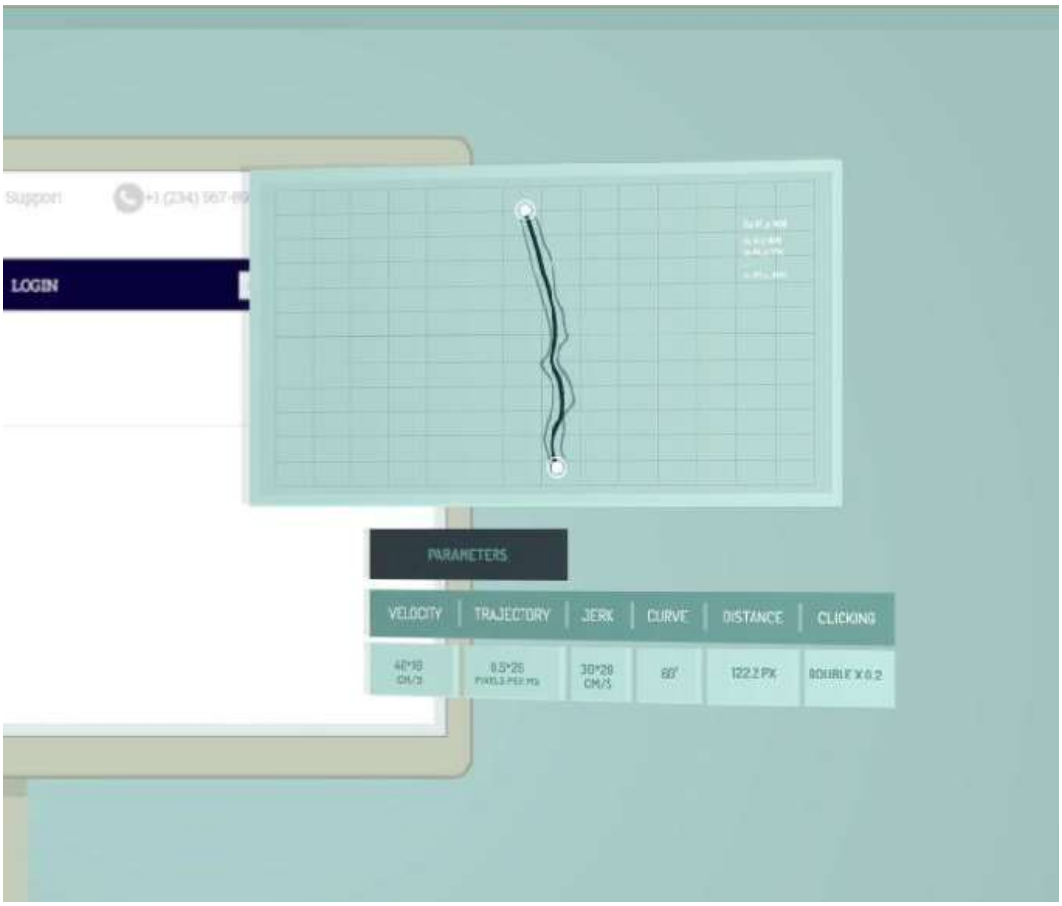
displayed by the client device by using, at least in part, by predicting the pixel distance pathlengths possible (*e.g.*, on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

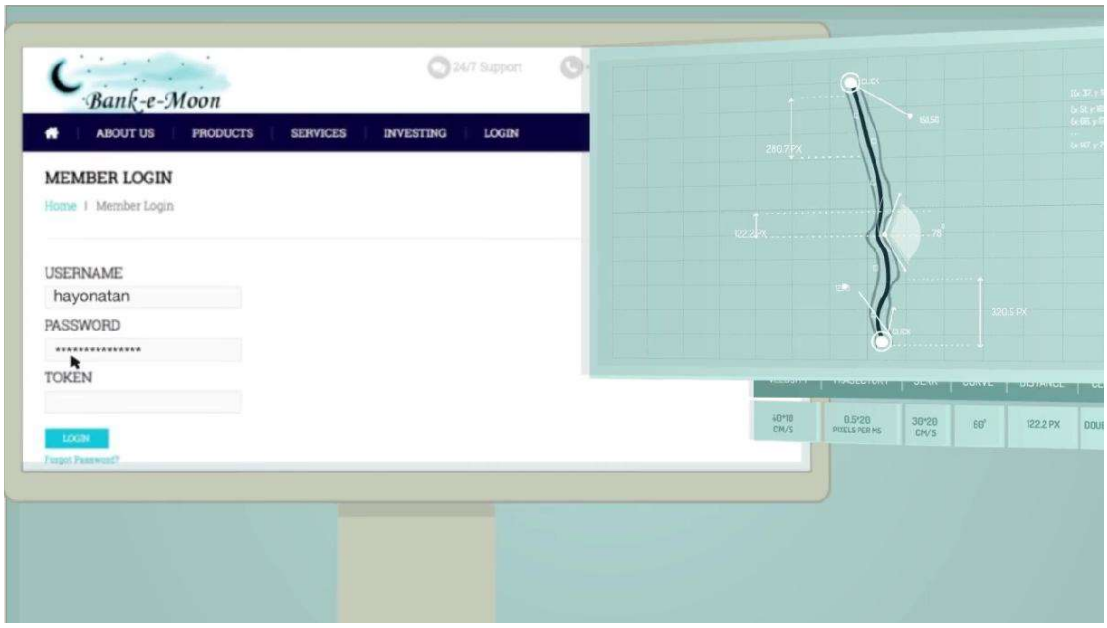
139. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates locations of rendered page geometry of the features and functions by using, at least in part, a distance of 122.2 pixels that is derived by subtracting the pixel locations of the two mouse clicks that select the two input boxes. Trusteer Pinpoint Detect predicts the pixel distance pathlengths possible (as an example, on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.

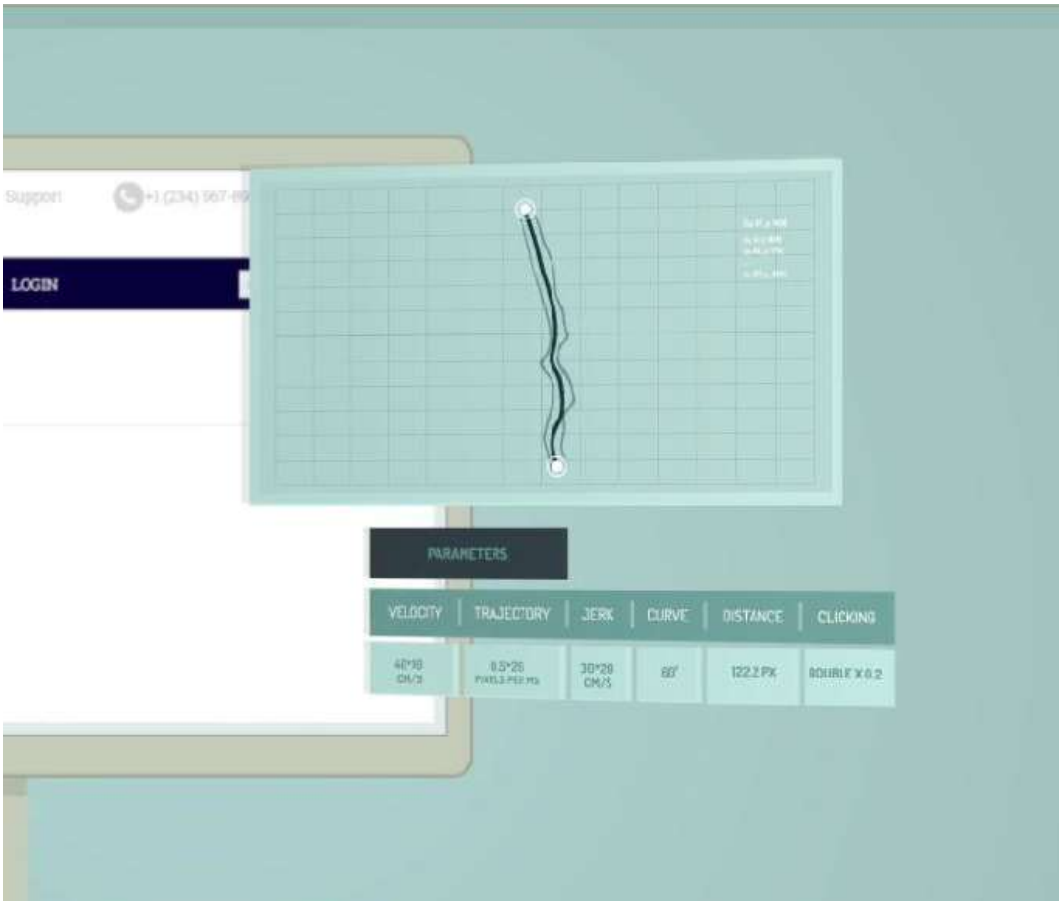

Bank-e-Moon
24/7 Support
ABOUT US
PRODUCTS
SERVICES
INVESTING
LOGIN
MEMBER LOGIN
Home | Member Login
USERNAME
hayonatan
PASSWORD
TOKEN
LOGIN
Forgot Password?
280.7 PX
122.2 PX
320.5 PX
40*10 CM/S
0.5*20 PIXELS PER MS
30*20 CM/S
60°
122.2 PX


Support
LOGIN
PARAMETERS
VELOCITY
TRAJECTORY
JERK
CURVE
DISTANCE
CLICKING
40*10 CM/S
0.5*20 PIXELS PER MS
30*20 CM/S
60°
122.2 PX
DOUBLE X 0.2

See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

140. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates relative locations between text, input boxes, buttons, and advertisements as displayed by the client device by using, at least in part, a relative (as opposed to absolute) distance of 122.2 PX (pixels) that is a measure of the distance between the click selecting the username input box and the click selecting the password input box. Pixels are a relative distance measuring unit that is tied to the number of pixels contained in the rendered page (*e.g.*, 4K image rendering is 4096 pixels by 2160 pixels). It is a relative size because the absolute size depends on the absolute geometry of the display screen used in the client's device and the pixel shape.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

COUNT I – DIRECT PATENT INFRINGEMENT OF THE '870 PATENT

141. SunStone realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

142. As the owner of the '870 Patent, SunStone holds all substantial rights in and to the '870Patent, including the right to exclude others from practicing its

patented inventions, the right to enforce the ’870 Patent, and the right to sue and recover damages for infringement of the ’870 Patent.

143. IBM has no authority or license to practice the inventions claimed in the ’870 Patent.

144. The ’870 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination by the USPTO.

145. IBM has infringed and continues to infringe at least claims 1-2, 4-11, 17-21, 37-39, and 42-43 of the ’870 Patent by, among other things, making, using, selling, testing, performing methods, offering for sale in the United States, and/or importing into the United States—without license or authority—including its own use and testing of, products, devices, or systems, including the IBM Security Trusteer Pinpoint Detect and IBM Security Trusteer Pinpoint Malware Detection Advanced Edition, and IBM Security Trusteer Mobile products (collectively the “Accused Products”) that fall within the scope of one or more claims of the ’870 Patent in violation of at least 35 U.S.C. § 271(a).

146. IBM’s infringing Accused Products include, without limitation, PinPoint Detect and Trusteer Mobile and other solutions with the same or similar features and functionality that satisfy each element of one or more asserted claims.

147. IBM's acts of making, using, importing, selling, and/or offering for sale Accused Products and services have been without the permission, consent, authorization, or license of SunStone.

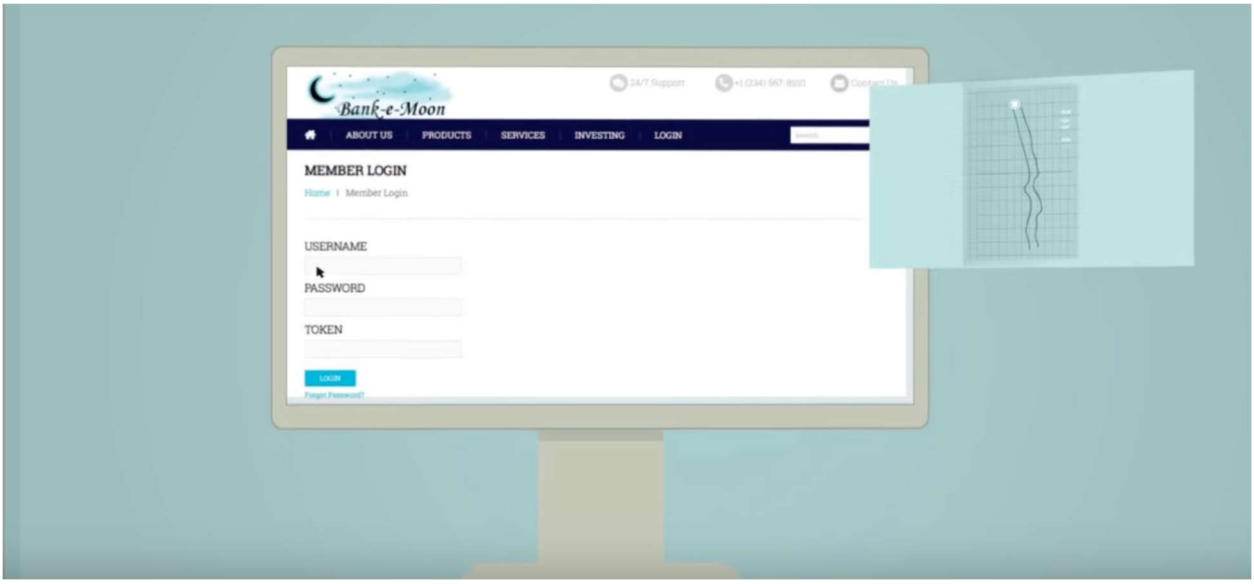
148. For example, the Accused Products embody the patented invention of the '870 Patent and infringe the '870 Patent because they practice at least a method comprising:

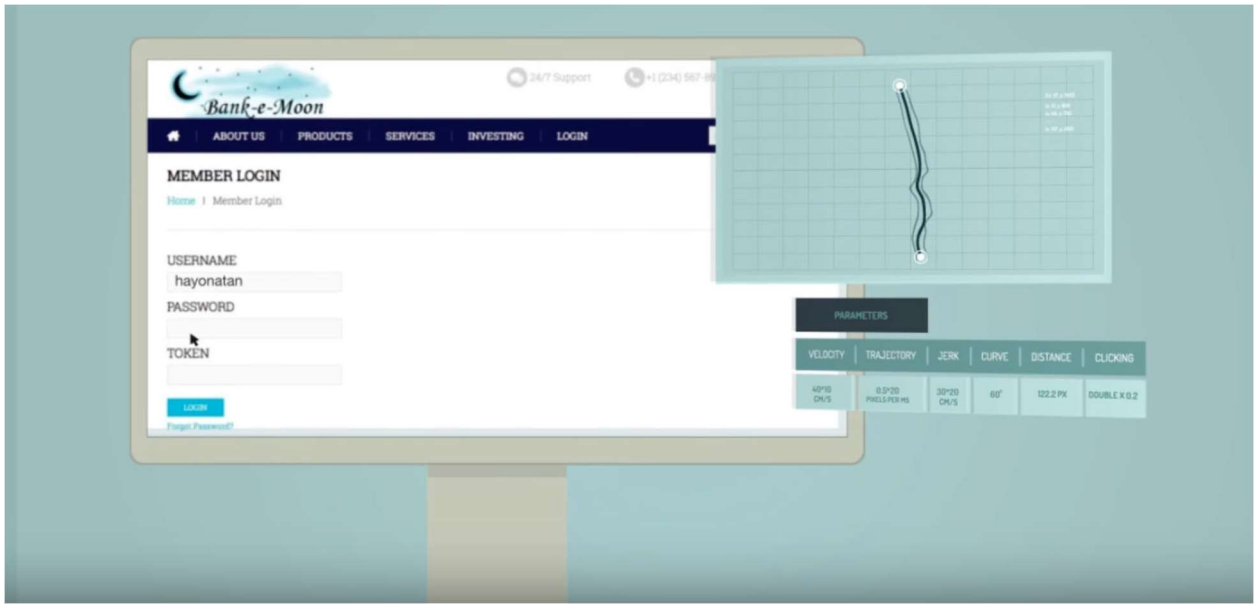
> selecting transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device;
>
> selecting presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed;
>
> transmitting at least one message including the presentation and transactional information from the server to the client device;
>
> determining a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information specified by the presentation information, and iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device;
>
> receiving the response message from the client device; and responsive to information in the response message not matching the prediction, providing an indication there is a malicious application affecting communications between the server and the client device,
>
> wherein the prediction is further determined based at least in part by at least one of: (a) estimating locations of rendered features and functions as displayed by the client device, (b) estimating locations of rendered page

> geometry of the features and functions, (c) estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device, (d) estimating a label of the presentation information, (e) estimating a utilization of a codeword set based on the presentation information and transactional information, and (f) estimating a utilization of a codeword set based on actions taken by at least one of the user and the client device.

'870 Patent, Claim 1.

149. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect software utilizes predictions based on one or more of estimating locations of rendered features and functions as displayed by the client device, estimating locations of rendered page geometry of the features and functions, estimating a label of the presentation information, and estimating a utilization of a codeword set based on the presentation information and transactional information.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4

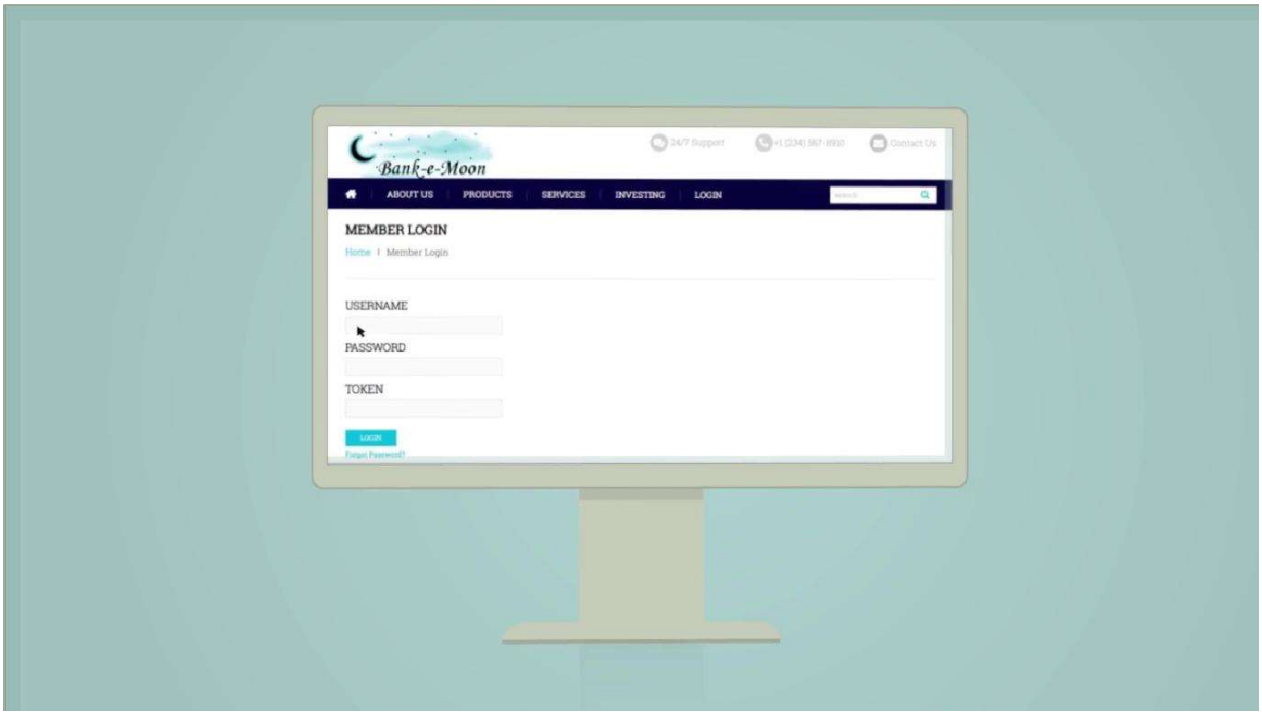
150. According to IBM, Trusteer Pinpoint Detect is deployed as a software as a service (SaaS) solution. It is designed to help organizations quickly and transparently establish digital identity trust. This can allow them to create a more seamless customer experience, without compromising on security. Trusteer Pinpoint Detect uses artificial intelligence and machine learning to help protect digital channels against account takeover and fraudulent transactions and can help detect end-user devices infected with high-risk malware. Trusteer Pinpoint Detect is a cloud-based solution that provides risk assessment for online identities to help differentiate between malicious users and true customers. *See* Ex. W, IBM, *Trusteer*

Pinpoint Detect Overview, *available at* https://www.ibm.com/us-en/marketplace/trusteer-pinpoint-detect.

151. Trusteer Pinpoint Detect is available for mobile solutions, Trusteer Mobile, which helps detect real-time device and session risks. According to IBM, Trusteer Pinpoint Detect helps maintain the integrity of the application in which it has been enabled by leveraging advanced analytics and real-time device risk detection. Trusteer Mobile assesses the device to determine if it is compromised such as by malware, remote access trojans, jailbroken/rooted detection, overlay attack evidence and SMS stealing apps. Additional cross-channel indicators are continuously processed leveraging advanced technologies such as behavioral anomalies, navigation discrepancies and phishing compromise. *See* Ex. X, IBM, *Mobile SDK*, *available at* https://www.ibm.com/us-en/marketplace/trusteer-mobile-sdk. Trusteer Mobile uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* *https://www.ibm.com/products/trusteer-pinpoint-detect/faq*.

152. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in Trusteer Pinpoint Detect, a server, such as, for example, the Bank-e-Moon server illustrated in the Behavioral Biometrics Demo Video, receives a request for the member login web page from the Client device. In response to that request, the server has selected the transactional information (hard information) to request from

the client. In the Bank-e-Moon demo provided by IBM, the server is requesting a "USERNAME," "PASSWORD," and "TOKEN."



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

153. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect next provides for selecting presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. For example, as shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the server has received a request for the

member login web page from the Client device. The presentation information was selected before sending the code to the client device.

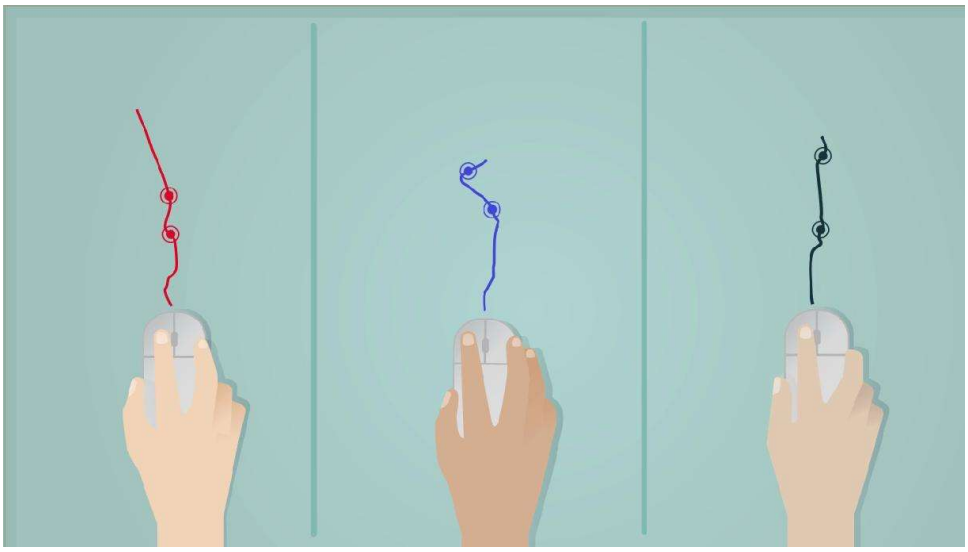
154. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect selects presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. Trusteer Pinpoint Detect accomplishes this by attaching mousemove event listener to the rendered page for the purposes of asking for clientX, clientY (*i.e.*, the X, Y coordinates of the mouse click). Trusteer Pinpoint Detect attaches mousedown mouseup click event listeners on the selected transactional fields – username and password. The event listener functions are re-polymorphed each session.

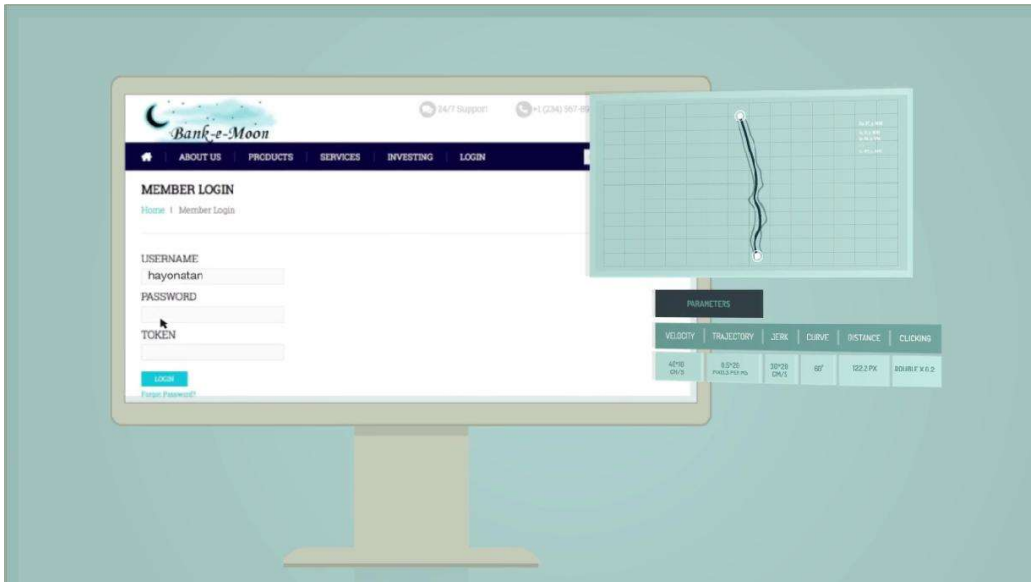
155. IBM inputs JavaScript into the client's web browser. According to IBM, Trusteer Pinpoint Detect works transparently, without the need for downloading executable files or plug-ins to the end user's computer. For web applications, Pinpoint uses code embedded into the webpage. For mobile applications, the organization's app uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

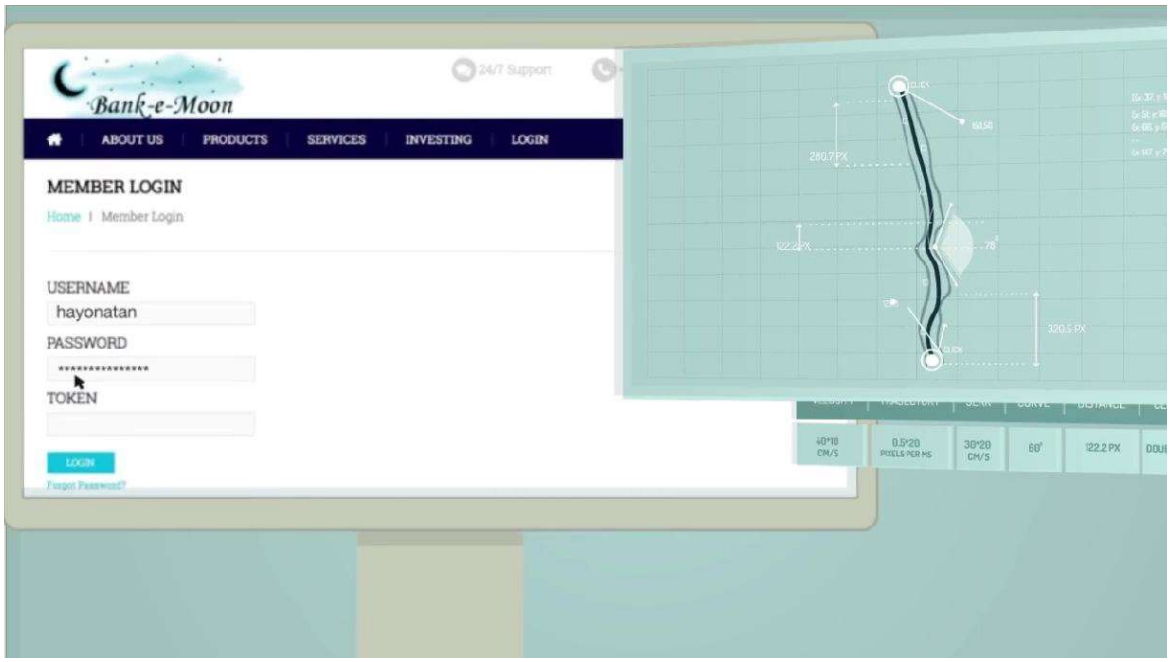
156. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect transmits at least one message including the presentation and transactional information from the server to the client device. This is illustrated by the displayed rendering of the information on the client's device.

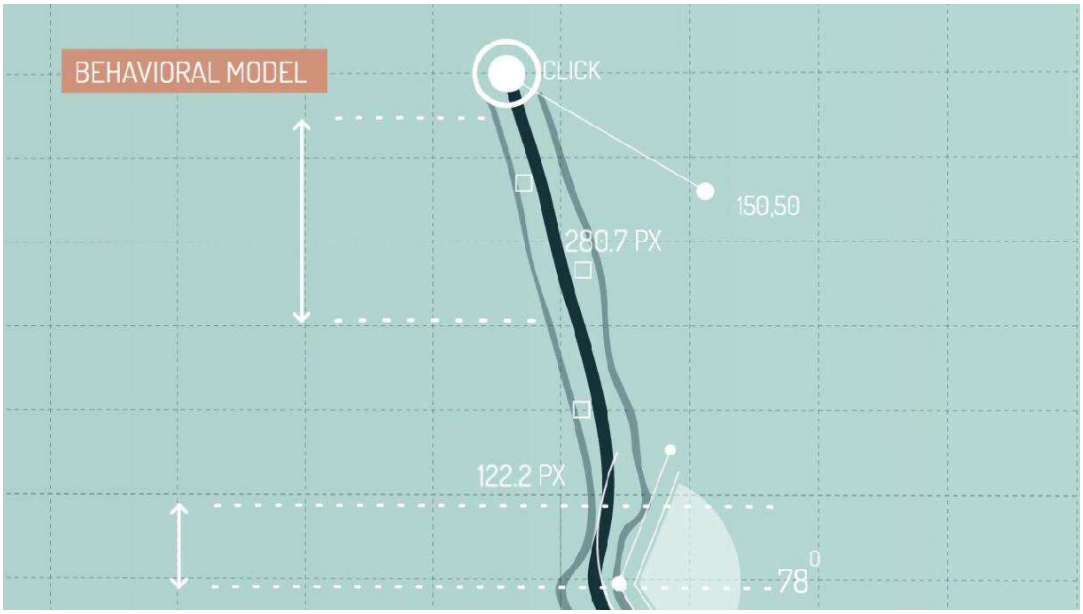
157. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect determines a prediction of a response message from a client device based on (i) the selected transactional information; (ii) how the client device is configured to render the transactional information specified by the presentation information, and (iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device. For example, Trusteer Pinpoint Detect tracks (in the response message) the mouse movements of the client mouse to determine a unique biometric signature, partly based on the starting and ending locations of the mouse. The predicted response signature for the client (stored in Trusteer Pinpoint Detect memory) is compared to the actual response signature (message from client). Trusteer Pinpoint Detect builds a behavioral biometric model that it expects to see for the client to be authenticated partly based on the rendered locations of the transactional (hard) information. The predicted response message for Trusteer Pinpoint Detect would include entering the client's correct username, mouse click order, mouse locations, number of clicks, and path shape parameters, followed by entering the client's

correct password. The measured path shape parameters include velocity, trajectory, jerk, curvature, and distance.









See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

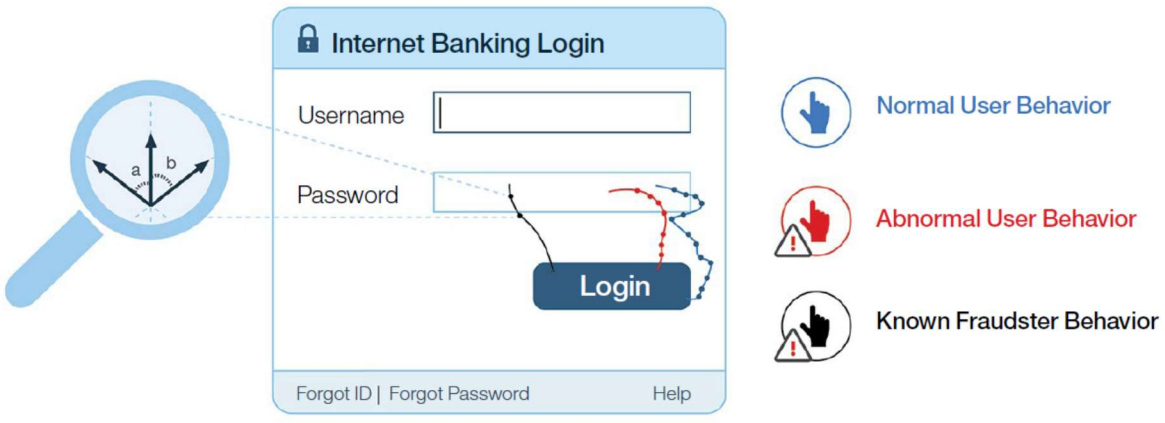
158. IBM accurately describes Trusteer Pinpoint Detect as follows:

IBM Security Trusteer Pinpoint™ Detect now incorporates behavioral biometric capabilities to provide dynamic, context-aware identity analytics that helps improve detection while preserving the user experience.

Built in conjunction with IBM Research labs, the solution's behavioral biometric capability uses machine learning to create a model based on patterns of mouse movements—from login through the entire application flow.

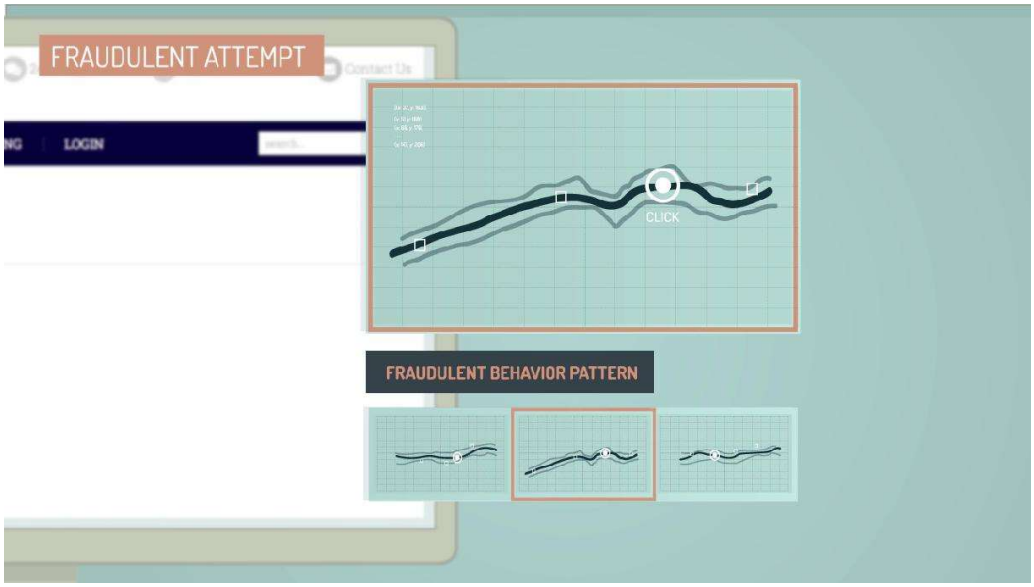
What angle does a user's mouse approach the login box? What direction does the user typically move the mouse? Mouse trajectory, velocity, curvature, jerk, and more are all analyzed.

The platform understands these subtle mouse movements in context and meaning, at astonishing speeds and volumes. It continuously and seamlessly learns user behavior across hundreds of millions of sessions and analyzes current online activity to detect unusual behavior across different devices, even comparing it against observed behavior of known fraudsters for even stronger evidence. If either abnormal user behavior or known fraudster behavior is detected by the platform's sophisticated algorithms, Trusteer Pinpoint Detect provides access management systems and security analysts with a recommended action in real time along with the detailed reasoning and session details so an action can be taken.



Ex. Y, IBM Security, *Thought Leadership White Paper, Shifting the balance of power with cognitive fraud detection*.

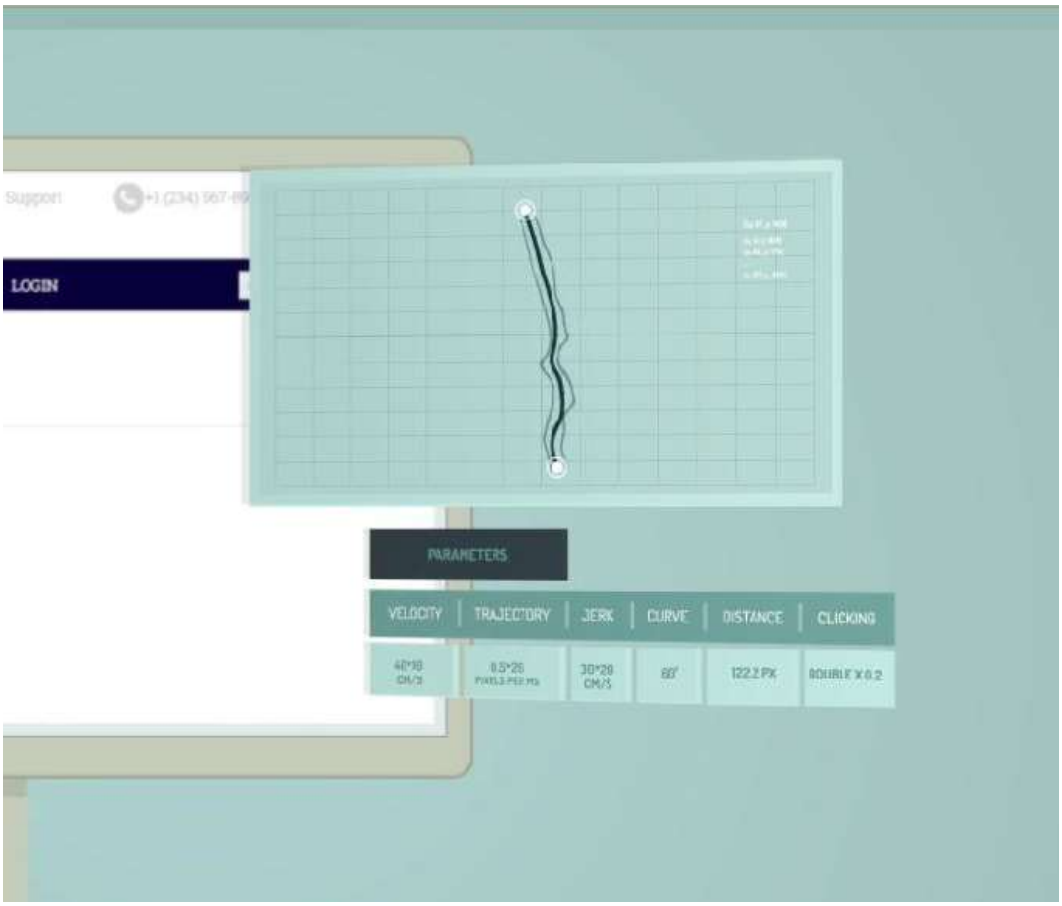
159. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect receives the response message from the client device; and responsive to the information in the response message not matching the prediction, provides an indication there is a malicious application affecting communications between the server and the client device. Trusteer Pinpoint Detect compares the client's mouse path and click locations (based on rendered and displayed transaction information) contained in the response message to the prediction. If there is a match, then the client is authenticated. If it does not match, or matches a known fraudulent behavior pattern, a fraudulent attempt is indicated.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

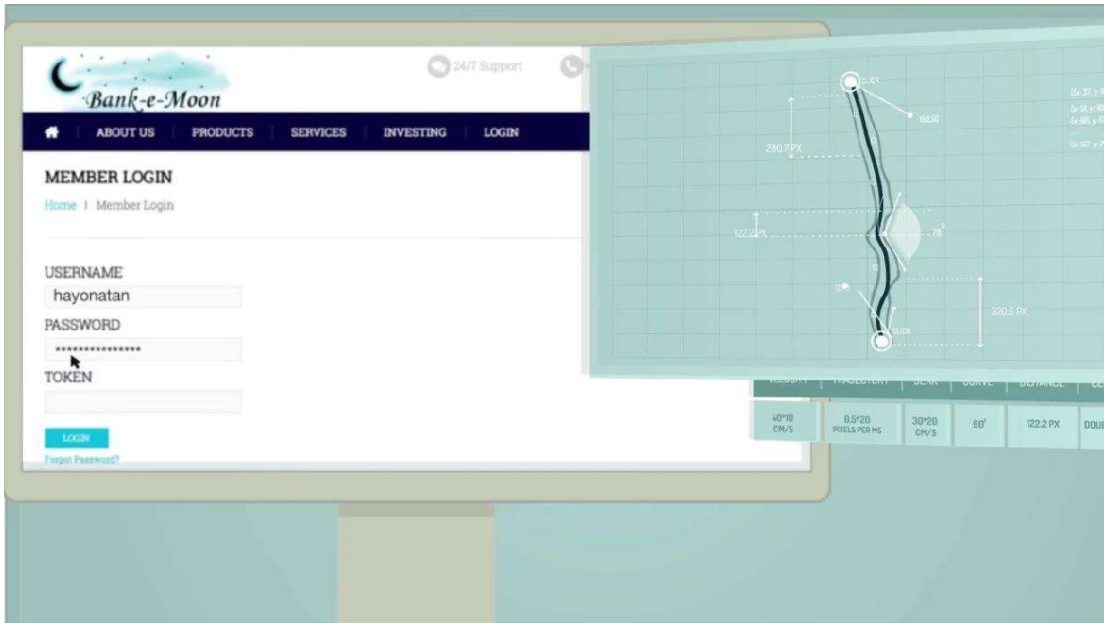
160. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates locations of rendered features and functions as

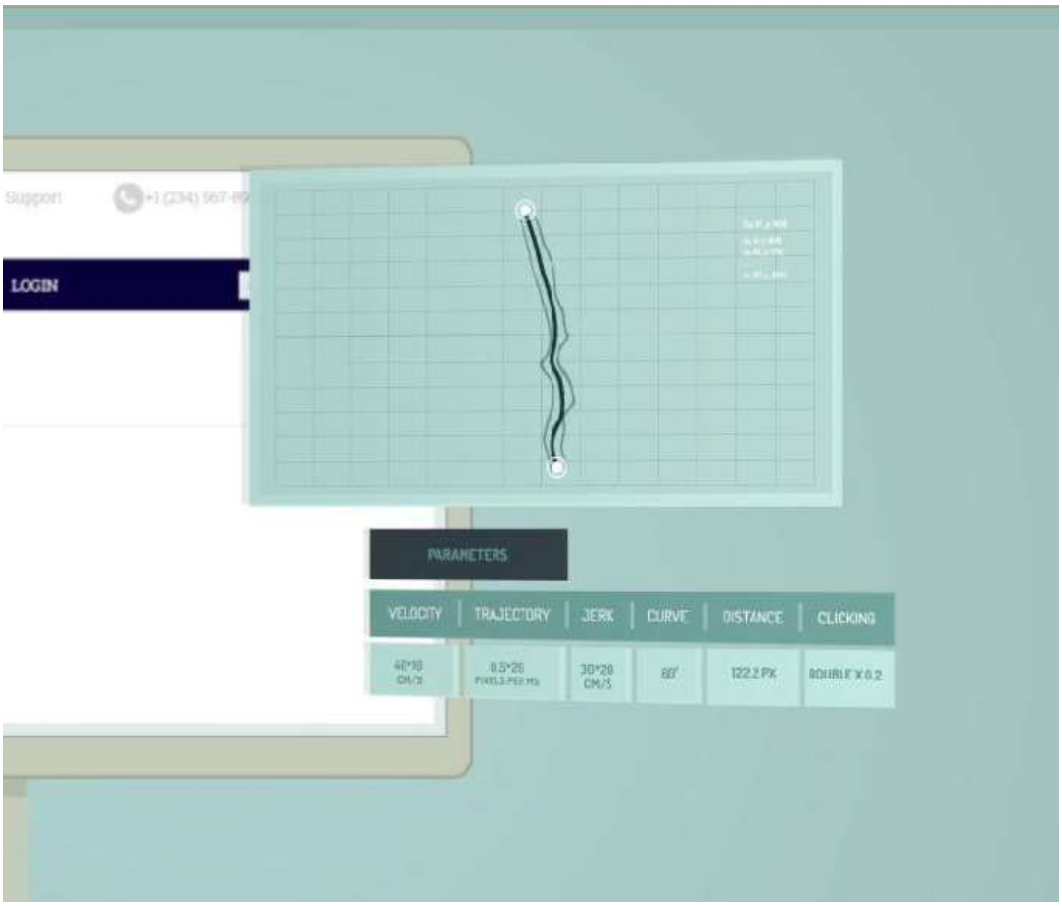
displayed by the client device by using, at least in part, by predicting the pixel distance pathlengths possible (*e.g.*, on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

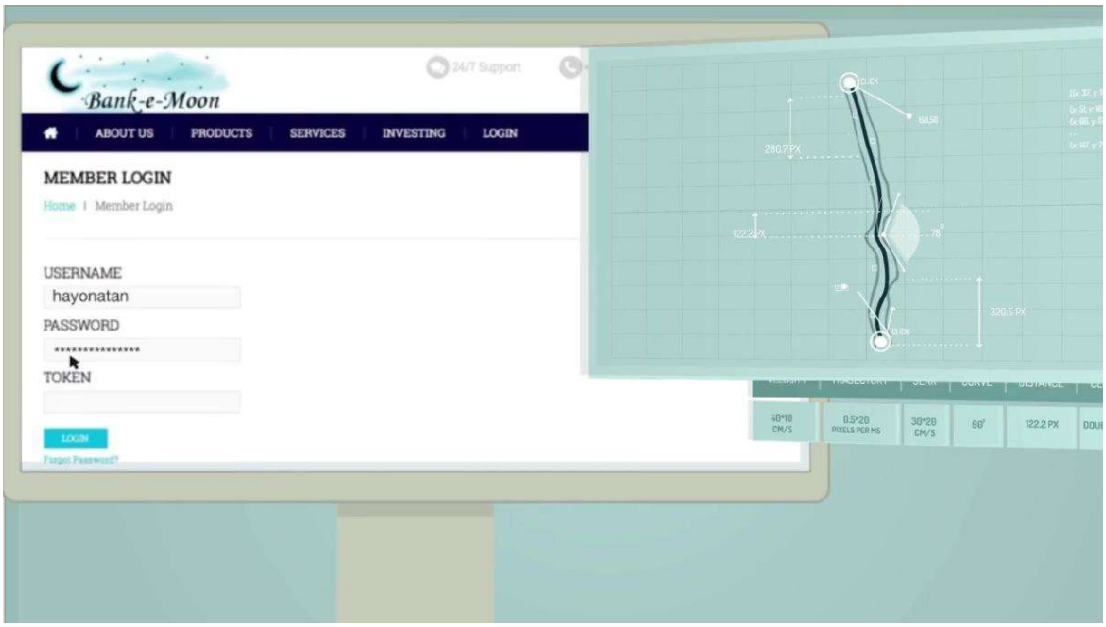
161. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates locations of rendered page geometry of the features and functions by using, at least in part, a distance of 122.2 pixels that is derived by subtracting the pixel locations of the two mouse clicks that select the two input boxes. Trusteer Pinpoint Detect predicts the pixel distance pathlengths possible (as an example, on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.

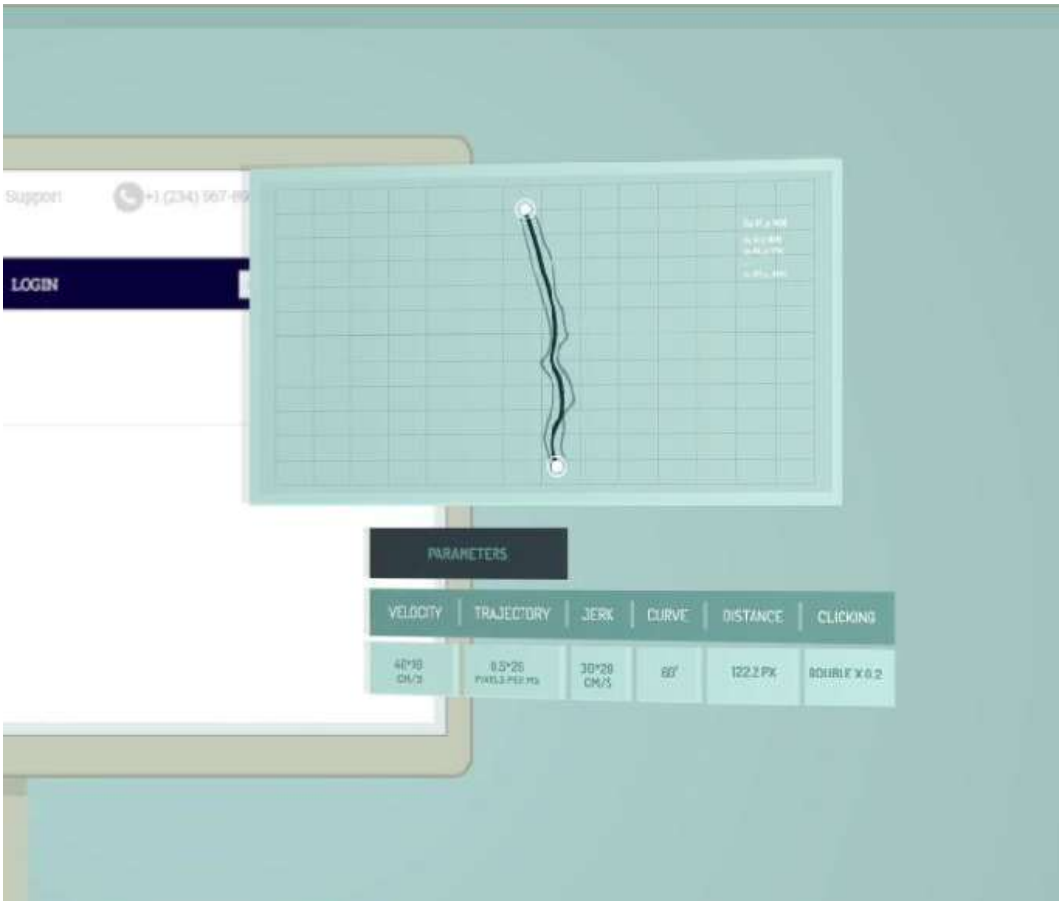

Bank-e-Moon
24/7 Support
ABOUT US
PRODUCTS
SERVICES
INVESTING
LOGIN
MEMBER LOGIN
Home | Member Login
USERNAME
hayonatan
PASSWORD
TOKEN
LOGIN
Forgot Password?
280.7 PX
320.5 PX
122.2 PX


LOGIN
PARAMETERS
VELOCITY
TRAJECTORY
JERK
CURVE
DISTANCE
CLICKING
122.2 PX

See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

162. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates relative locations between text, input boxes, buttons, and advertisements as displayed by the client device by using, at least in part, a relative (as opposed to absolute) distance of 122.2 PX (pixels) that is a measure of the distance between the click selecting the username input box and the click selecting the password input box. Pixels are a relative distance measuring unit that is tied to the number of pixels contained in the rendered page (*e.g.*, 4K image rendering is 4096 pixels by 2160 pixels). It is a relative size because the absolute size depends on the absolute geometry of the display screen used in the client's device and the pixel shape.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

163. The Accused Products satisfy each and every element of each asserted claim of the '870 Patent either literally or under the doctrine of equivalents.

164. IBM's infringing activities are and have been without authority or license under the '870 Patent.

165. As a result of IBM's unlawful activities, SunStone has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, SunStone is entitled to preliminary and/or permanent injunctive relief.

166. IBM's infringement of the '870 Patent has injured and continues to injure SunStone in an amount to be proven at trial.

167. At least as early as July 2, 2016, Nick Coleman, IBM's Global Head Cyber Security Intelligence, requested a demonstration of SunStone's technology, as described in the '870 Patent.

168. SunStone is informed and believes that despite IBM's knowledge of the '870 Patent and SunStone's patented technology, IBM made the deliberate decision(s) to sell products and services that it knew infringe SunStone's '870 Patent.

169. SunStone is informed and believes that IBM has undertaken no efforts to avoid infringement of the '870 Patent, despite IBM's knowledge and understanding that IBM's products and services infringe these patents. Thus, IBM's infringement of '870 Patent is willful and egregious, warranting enhancement of damages.

170. As such, IBM has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously to engage in acts of infringement of the '870

Patent, justifying an award to SunStone of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II – INDUCED PATENT INFRINGEMENT OF THE '870 PATENT

171. SunStone realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

172. As set forth above, IBM is liable for indirect infringement under 35 U.S.C. § 271(b) of at least claims 1-2, 4-11, 17-21, 37-39, and 42-43 of the '870 Patent at least as early as service of the Original Complaint on November 9, 2020, because it knowingly encourages, aids, and directs others (*e.g.*, end users and customers) to use and operate the Accused Products in an infringing manner and to perform the claimed methods of the '870 Patent.

173. At least as early as July 2, 2016, Nick Coleman, IBM's Global Head Cyber Security Intelligence, requested a demonstration of SunStone's technology, as described in the '870 Patent.

174. Since at least as early as service of the Original Complaint on November 9, 2020, IBM has had knowledge of the '870 Patent. Since that time, IBM has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including IBM's customers, to use the Accused Products in a manner that infringe the '870 Patent. This is evident when IBM encourages and instructs customers and other end users in the use and operation

of the Accused Products via advertisement, technical material, instructional material, and otherwise.

175. IBM specifically intends the Accused Products to be used and operated to infringe one or more claims, including at least claims 1-2, 4-11, 17-21, 37-39, and 42-43 of the ’870 Patent.

176. IBM encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

177. As detailed above, IBM has instructed its customers to use the accused methods and Accused Products in an infringing manner.

178. IBM’s analysis and knowledge of the ’870 Patent combined with its ongoing activity demonstrates IBM’s knowledge and intent that the identified features of its Accused Products be used to infringe the ’870 Patent.

179. IBM’s knowledge of the ’870 Patent and SunStone’s infringement allegations against IBM combined with its knowledge of the Accused Products and how they are used to infringe the ’870 Patent, consistent with IBM’s promotions and instructions, demonstrate IBM’s specific intent to induce PinPoint Detect and Trusteer Mobile users to infringe the ’870 Patent.

180. SunStone is entitled to recover from IBM compensation in the form of monetary damages suffered as a result of IBM’s infringement in an amount that

cannot be less than a reasonable royalty together with interest and costs as fixed by this Court.

COUNT III – DIRECT PATENT INFRINGEMENT OF THE '682 PATENT

181. SunStone realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

182. As the owner of the '682 Patent, SunStone holds all substantial rights in and to the '682Patent, including the right to exclude others from practicing its patented inventions, the right to enforce the '682 Patent, and the right to sue and recover damages for infringement of the '682 Patent.

183. IBM has no authority or license to practice the inventions claimed in the '682 Patent.

184. The '682 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code after a full and fair examination by the USPTO.

185. IBM has infringed and continues to infringe at least claims 1-11 and 21-29 of the '682 Patent by, among other things, making, using, selling, testing, performing methods, offering for sale in the United States, and/or importing into the United States—without license or authority—including its own use and testing of, products, devices, or systems, including the IBM Security Trusteer Pinpoint Detect and IBM Security Trusteer Pinpoint Malware Detection Advanced Edition, and IBM

Security Trusteer Mobile products (collectively the "Accused Products") that fall within the scope of one or more claims of the '682 Patent in violation of at least 35 U.S.C. § 271(a).

186. IBM's infringing Accused Products include, without limitation, PinPoint Detect and Trusteer Mobile and other solutions with the same or similar features and functionality that satisfy each element of one or more asserted claims.

187. IBM's acts of making, using, importing, selling, and/or offering for sale Accused Products and services have been without the permission, consent, authorization, or license of SunStone.

188. For example, the Accused Products embody the patented invention of the '682 Patent and infringe the '682 Patent because they practice at least a method comprising:

selecting, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device;

selecting, via the processor, presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed;

transmitting, via the processor, at least one message including the presentation and transactional information from the server to the client device;

determining, via the processor, a prediction of a response message from the client device based on i) the selected transactional information, ii) how the client device is configured to render the transactional information

specified by the presentation information, and iii) expected response information associated with the transactional information that is expected to be provided by a user of the client device;

receiving, in the processor, the response message from the client device; and

responsive to information in the response message not matching the prediction, providing, via the processor, an indication there is a malicious application affecting communications between the server and the client device,

wherein the prediction is further determined by the processor based at least in part by estimating at least one location of at least one rendered feature or function as displayed by the client device,

wherein the presentation information includes at least one of protocol information, formatting information, positional information, rendering information, style information, transmission encoding information, information describing how different layers of a style sheet are to be rendered by the client device, or information changing a definition of a function in a code library at the client device, and

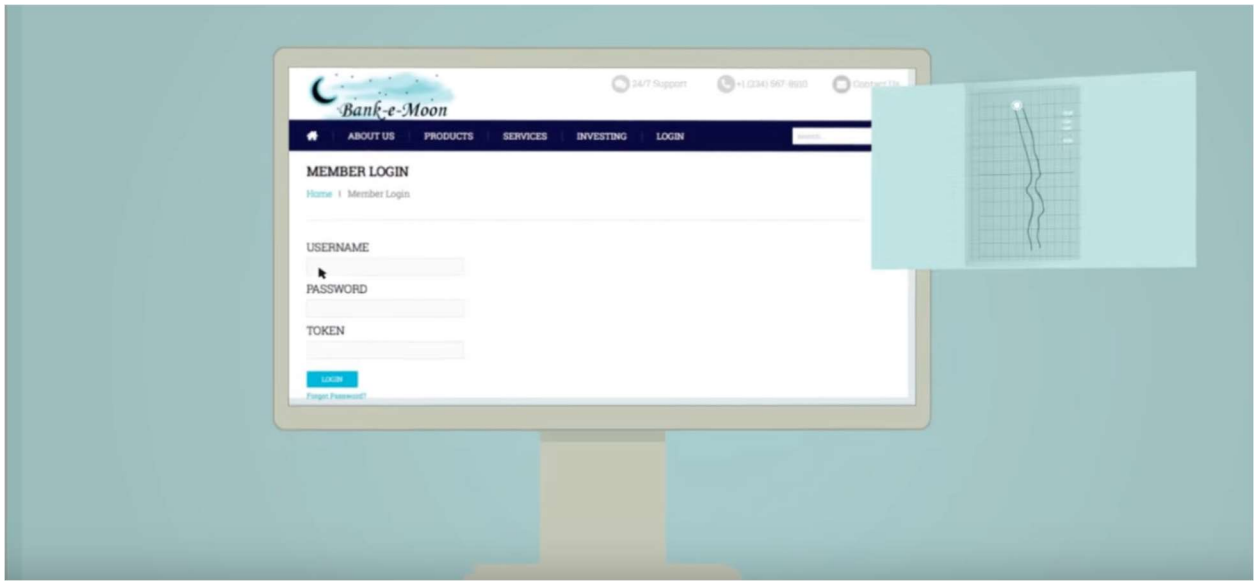
wherein the transactional information includes at least one of text, data, pictorial information, image information, information requested by the server to perform a service for the client device, authentication information, refinement information on a type of service requested by the client device, financial information, or data management information.

'682 Patent, Claim 1.

189. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the Accused Products perform a method via a processor. The Accused Products provide a method for validating communications in an open architecture system. Reference to Pinpoint Detect is not intended to exclude any accused IBM Trusteer

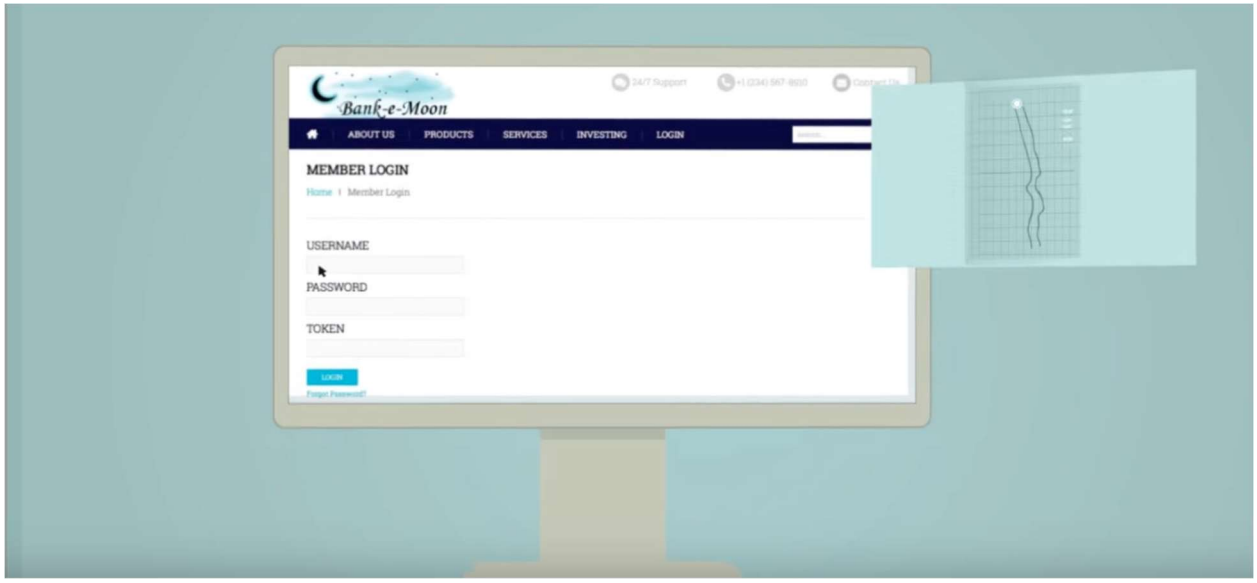
network security method or system. The Accused Products and Pinpoint Detect include at least IBM Security Trusteer Pinpoint products and systems, including at least IBM Security Trusteer Pinpoint Detect and IBM Security Trusteer Pinpoint Malware Detection Advanced Edition, and IBM Security Trusteer Mobile.

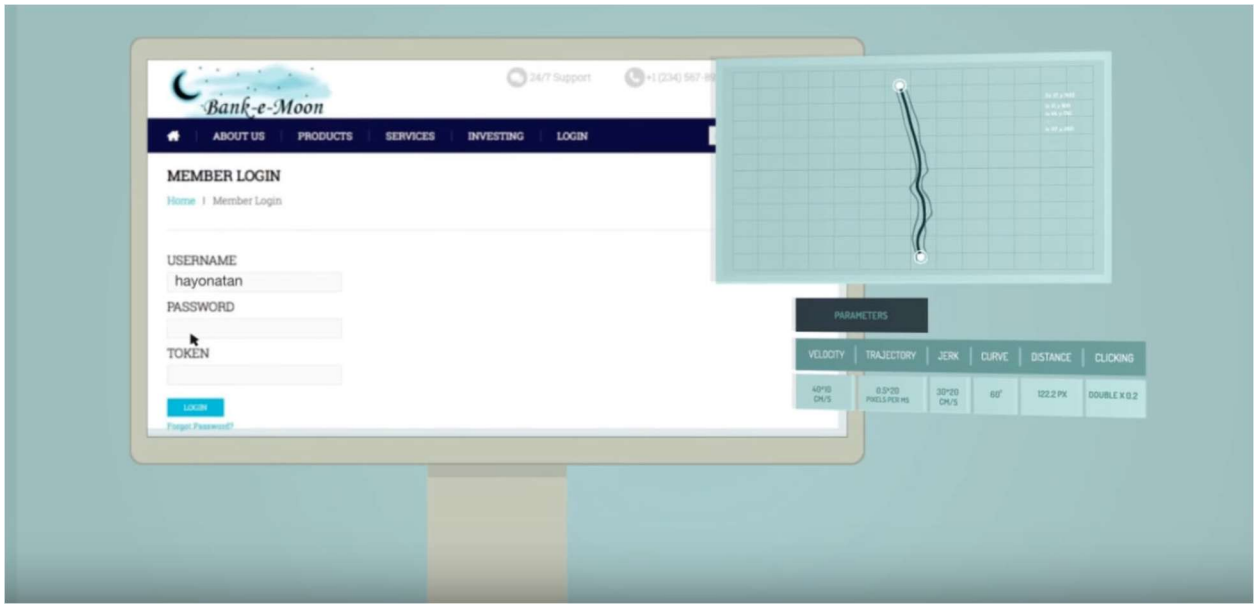
190. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, IBM uses the term "behavioral biometrics" to describe relevant features of the Accused Products. IBM's use of the term "behavioral biometrics" has evolved from the identification of a particular user by comparison to that user's prior activities to the analysis of a user's interaction(s) (response) with a purposefully altered application by comparing aspects of that interaction (response) to one or more predicted responses of a generic class of legitimate users.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

191. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect software utilizes predictions based on, at least, estimating at least one location of at least one rendered feature or function as displayed by the client device. For example, the Accused Products work as a cloud-based solution, delivering real-time threat data allowing for counter-attacks or control of a fraudulent incident. The Accused Products continuously authenticate a customer's identity by monitoring activity.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

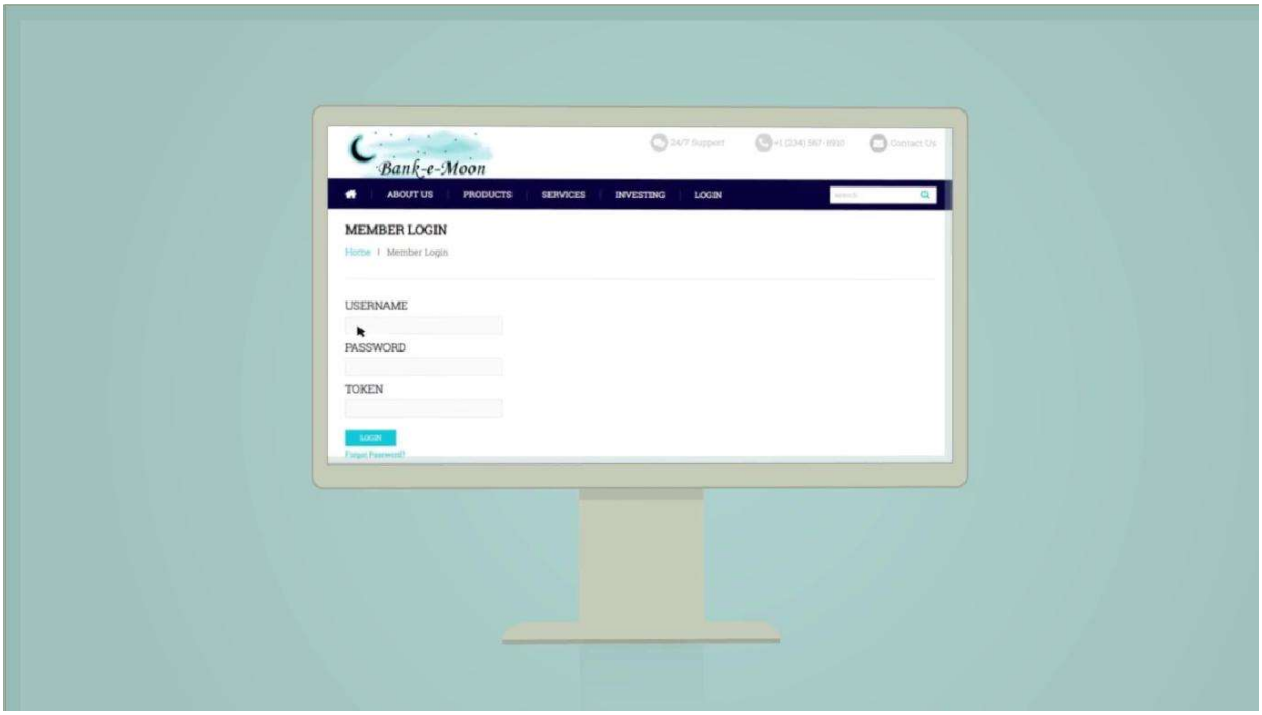
192. According to IBM, Trusteer Pinpoint Detect is deployed as a software as a service (SaaS) solution. It is designed to help organizations quickly and transparently establish digital identity trust. This can allow them to create a more seamless customer experience, without compromising on security. Trusteer Pinpoint Detect uses artificial intelligence and machine learning to help protect digital channels against account takeover and fraudulent transactions and can help detect end-user devices infected with high-risk malware. Trusteer Pinpoint Detect is a cloud-based solution that provides risk assessment for online identities to help differentiate between malicious users and true customers. *See* Ex. W, IBM, *Trusteer*

Pinpoint Detect Overview, *available at* https://www.ibm.com/us-en/marketplace/trusteer-pinpoint-detect.

193. Trusteer Pinpoint Detect is available for mobile solutions, Trusteer Mobile, which helps detect real-time device and session risks. According to IBM, Trusteer Pinpoint Detect helps maintain the integrity of the application in which it has been enabled by leveraging advanced analytics and real-time device risk detection. Trusteer Mobile assesses the device to determine if it is compromised such as by malware, remote access trojans, jailbroken/rooted detection, overlay attack evidence and SMS stealing apps. Additional cross-channel indicators are continuously processed leveraging advanced technologies such as behavioral anomalies, navigation discrepancies and phishing compromise. *See* Ex. X, IBM, *Mobile SDK*, *available at* https://www.ibm.com/us-en/marketplace/trusteer-mobile-sdk. Trusteer Mobile uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

194. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in Trusteer Pinpoint Detect, a server, such as, for example, the Bank-e-Moon server illustrated in the Behavioral Biometrics Demo Video, receives a request for the member login web page from the Client device. In response to that request, the server has selected the transactional information (hard information) to request from

the client. In the Bank-e-Moon demo provided by IBM, the server is requesting a "USERNAME," "PASSWORD," and "TOKEN."



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

195. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect next provides for selecting presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. For example, as shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the server has received a request for the

member login web page from the Client device. The presentation information was selected before sending the code to the client device.

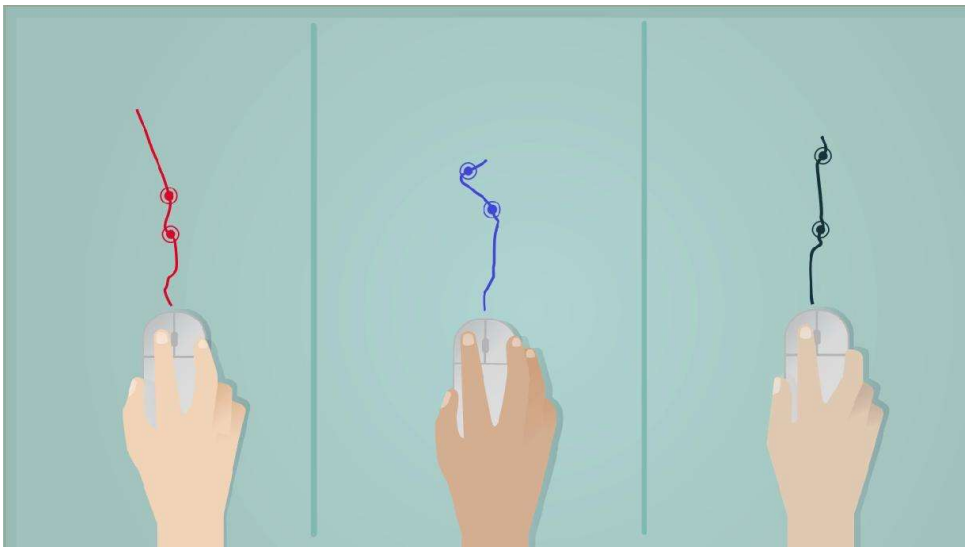
196. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect selects presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. Trusteer Pinpoint Detect accomplishes this by attaching mousemove event listener to the rendered page for the purposes of asking for clientX, clientY (*i.e.*, the X, Y coordinates of the mouse click). Trusteer Pinpoint Detect attaches mousedown mouseup click event listeners on the selected transactional fields – username and password. The event listener functions are re-polymorphed each session.

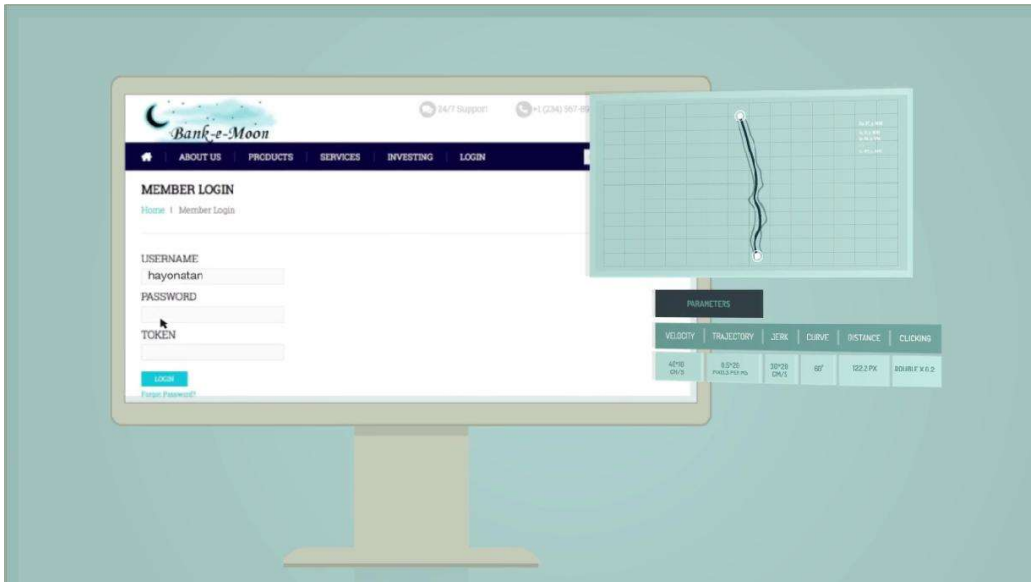
197. IBM inputs JavaScript into the client's web browser. According to IBM, Trusteer Pinpoint Detect works transparently, without the need for downloading executable files or plug-ins to the end user's computer. For web applications, Trusteer Pinpoint Detect uses code embedded into the webpage. For mobile applications, the organization's app uses the IBM Trusteer Mobile SDK. *See* Ex. R, IBM, *IBM Security Trusteer Pinpoint Detect*, *available at* https://www.ibm.com/products/trusteer-pinpoint-detect/faq.

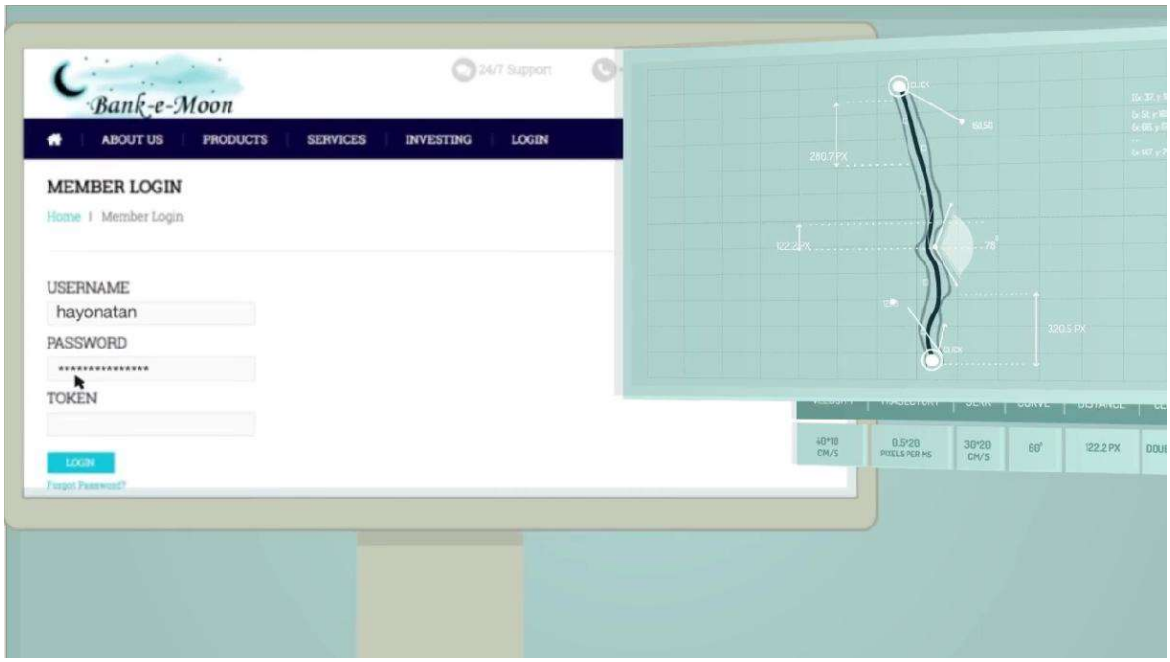
198. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect transmits at least one message including the presentation and transactional information from the server to the client device. This is illustrated by the displayed rendering of the information on the client's device.

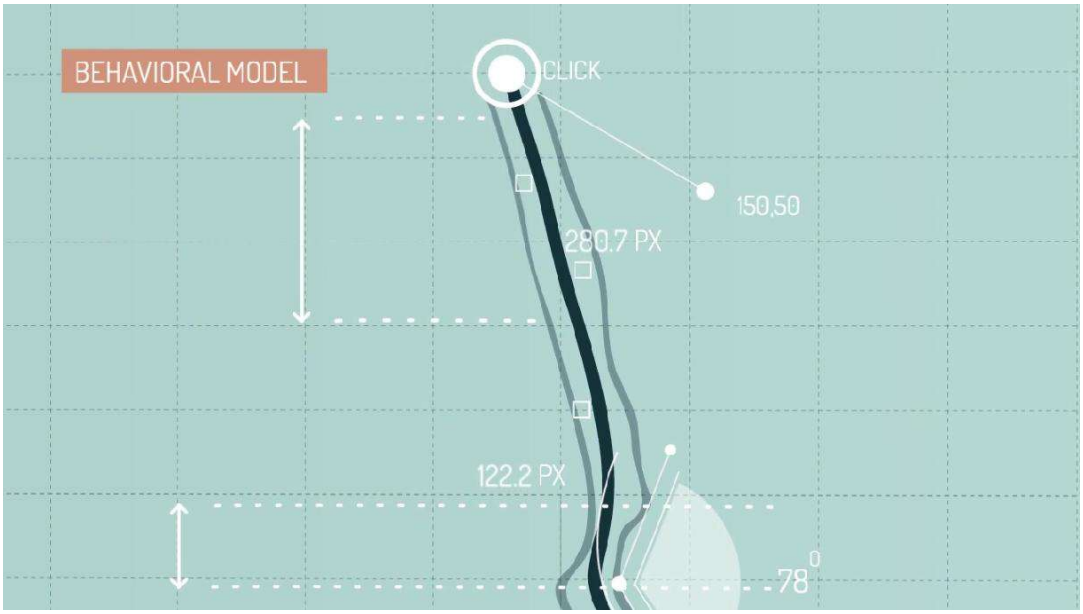
199. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect determines a prediction of a response message from a client device based on (i) the selected transactional information, (ii) how the client device is configured to render the transactional information specified by the presentation information, and (iii) expected response information associated with the transactional information that is expected to be provided by a user of the client device. For example, Trusteer Pinpoint Detect tracks (in the response message) the mouse movements of the client mouse to determine a unique biometric signature, partly based on the starting and ending locations of the mouse. The predicted response signature for the client (stored in Trusteer Pinpoint Detect memory) is compared to the actual response signature (message from client). Trusteer Pinpoint Detect builds a behavioral biometric model that it expects to see for the client to be authenticated partly based on the rendered locations of the transactional (hard) information. The predicted response message for Trusteer Pinpoint Detect would include entering the client's correct username, mouse click order, mouse locations, number of clicks, and path shape parameters, followed by entering the client's

correct password. The measured path shape parameters include velocity, trajectory, jerk, curvature, and distance.









See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

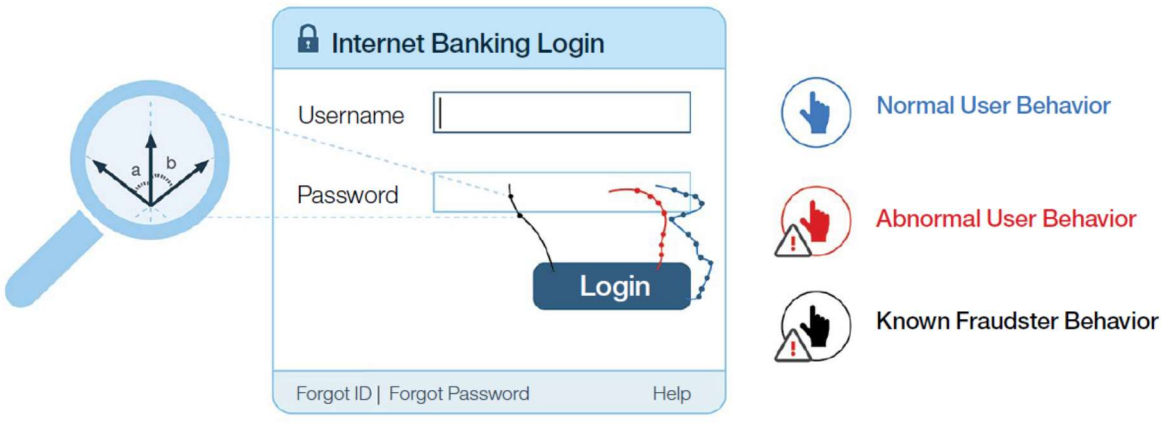
200. IBM accurately describes Trusteer Pinpoint Detect as follows:

IBM Security Trusteer Pinpoint™ Detect now incorporates behavioral biometric capabilities to provide dynamic, context-aware identity analytics that helps improve detection while preserving the user experience.

Built in conjunction with IBM Research labs, the solution's behavioral biometric capability uses machine learning to create a model based on patterns of mouse movements—from login through the entire application flow.

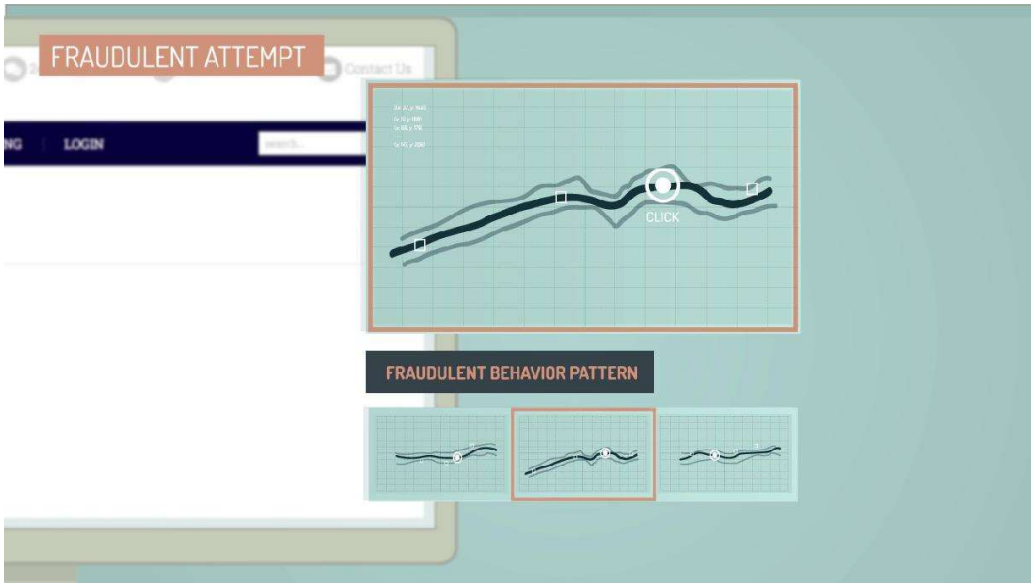
What angle does a user's mouse approach the login box? What direction does the user typically move the mouse? Mouse trajectory, velocity, curvature, jerk, and more are all analyzed.

The platform understands these subtle mouse movements in context and meaning, at astonishing speeds and volumes. It continuously and seamlessly learns user behavior across hundreds of millions of sessions and analyzes current online activity to detect unusual behavior across different devices, even comparing it against observed behavior of known fraudsters for even stronger evidence. If either abnormal user behavior or known fraudster behavior is detected by the platform's sophisticated algorithms, Trusteer Pinpoint Detect provides access management systems and security analysts with a recommended action in real time along with the detailed reasoning and session details so an action can be taken.



Ex. Y, IBM Security, *Thought Leadership White Paper, Shifting the balance of power with cognitive fraud detection*.

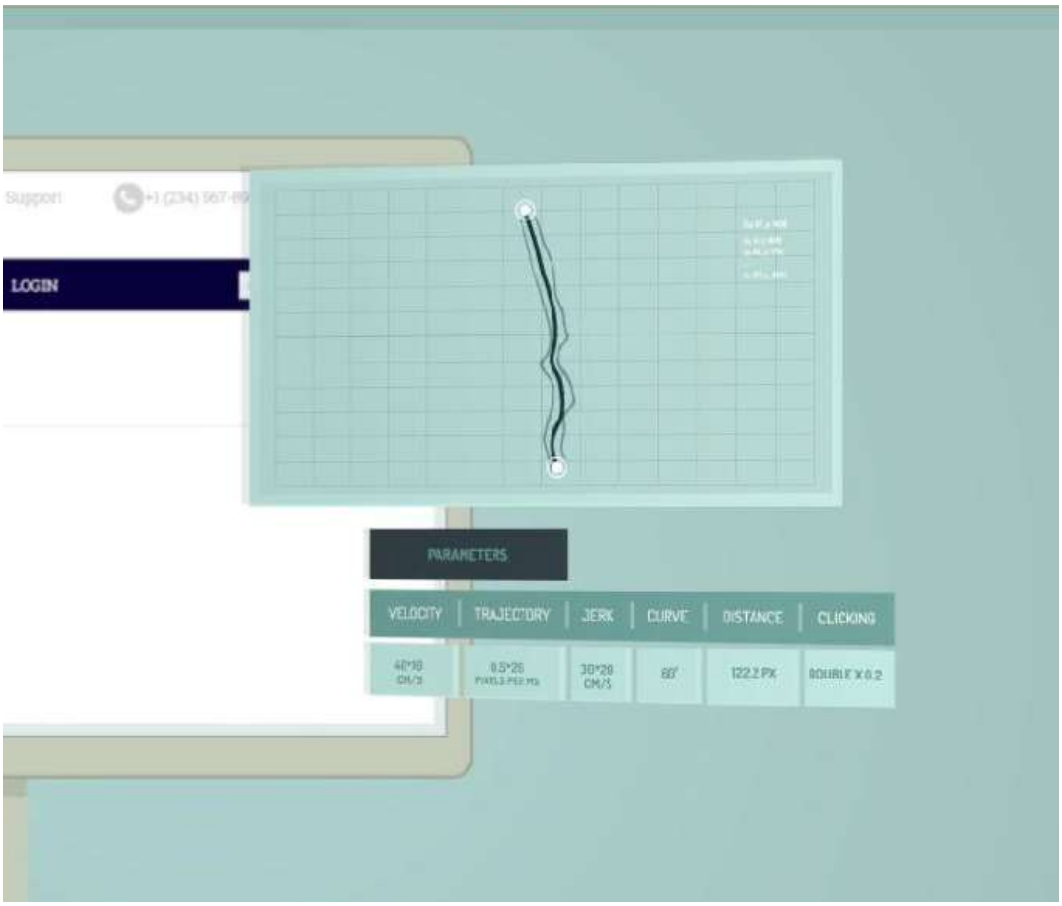
201. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect receives the response message from the client device; and responsive to the information in the response message not matching the prediction, provides an indication there is a malicious application affecting communications between the server and the client device. Trusteer Pinpoint Detect compares the client's mouse path and click locations (based on rendered and displayed transaction information) contained in the response message to the prediction. If there is a match, then the client is authenticated. If it does not match, or matches a known fraudulent behavior pattern, a fraudulent attempt is indicated.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

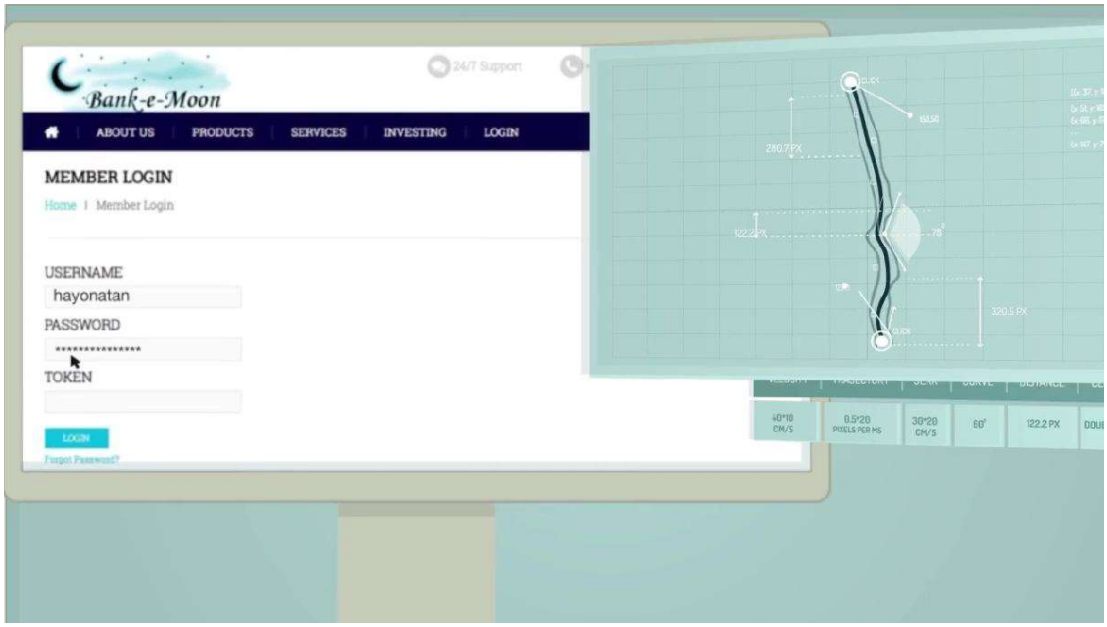
202. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in Trusteer Pinpoint Detect, the prediction is further determined by the processor

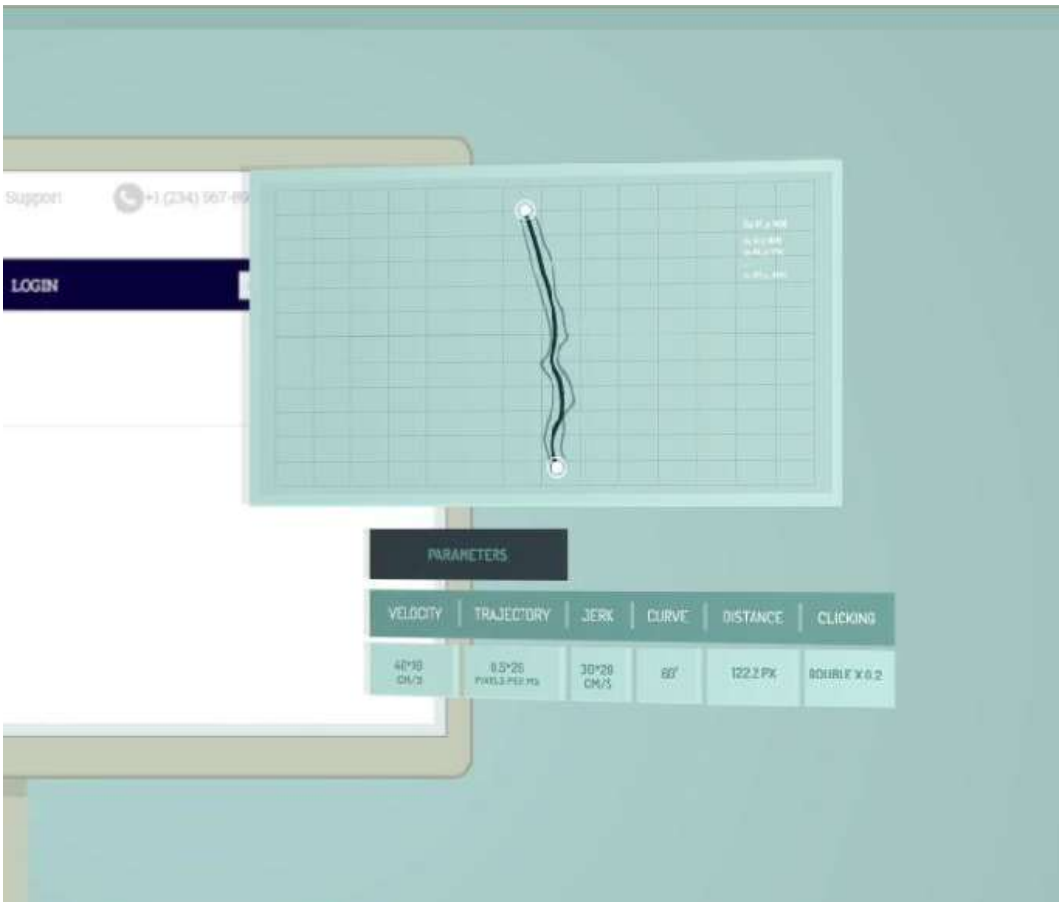
based at least in part by estimating at least one location of at least one rendered feature or function as displayed by the client device. For example, the Accused Products estimate locations of rendered features and functions as displayed by the client device by using, at least in part, by predicting the pixel distance pathlengths possible (e.g., on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

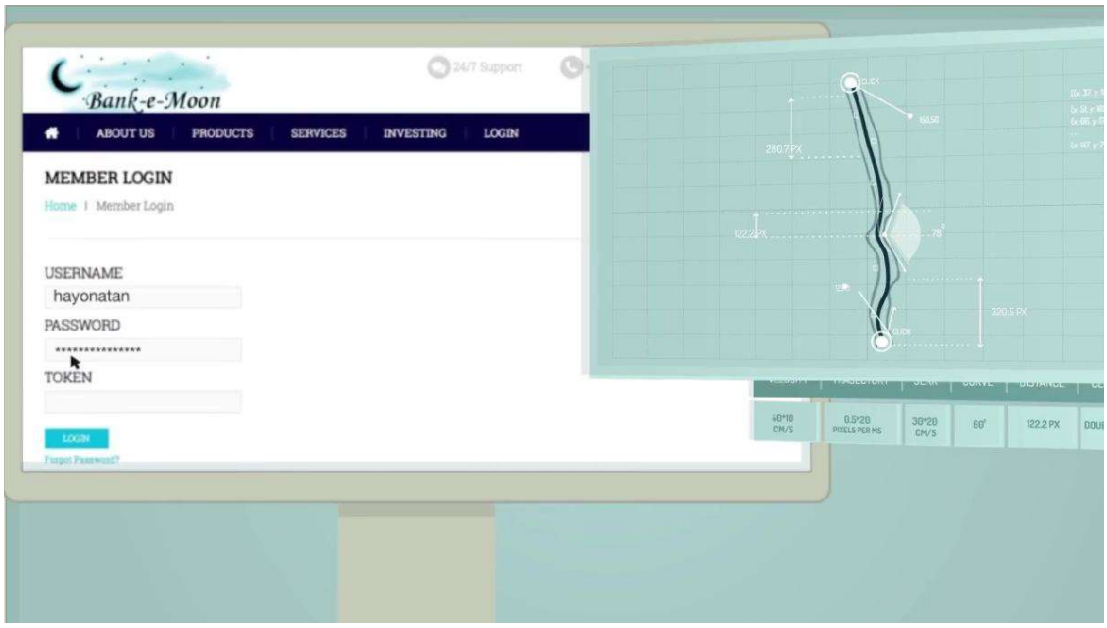
203. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates locations of rendered page geometry of the features and functions by using, at least in part, a distance of 122.2 pixels that is derived by subtracting the pixel locations of the two mouse clicks that select the two input boxes. Trusteer Pinpoint Detect predicts the pixel distance pathlengths possible (as an example, on the client's device for a 2K or 4K display) for the two mouse clicks needed to select the USERNAME and PASSWORD input boxes.

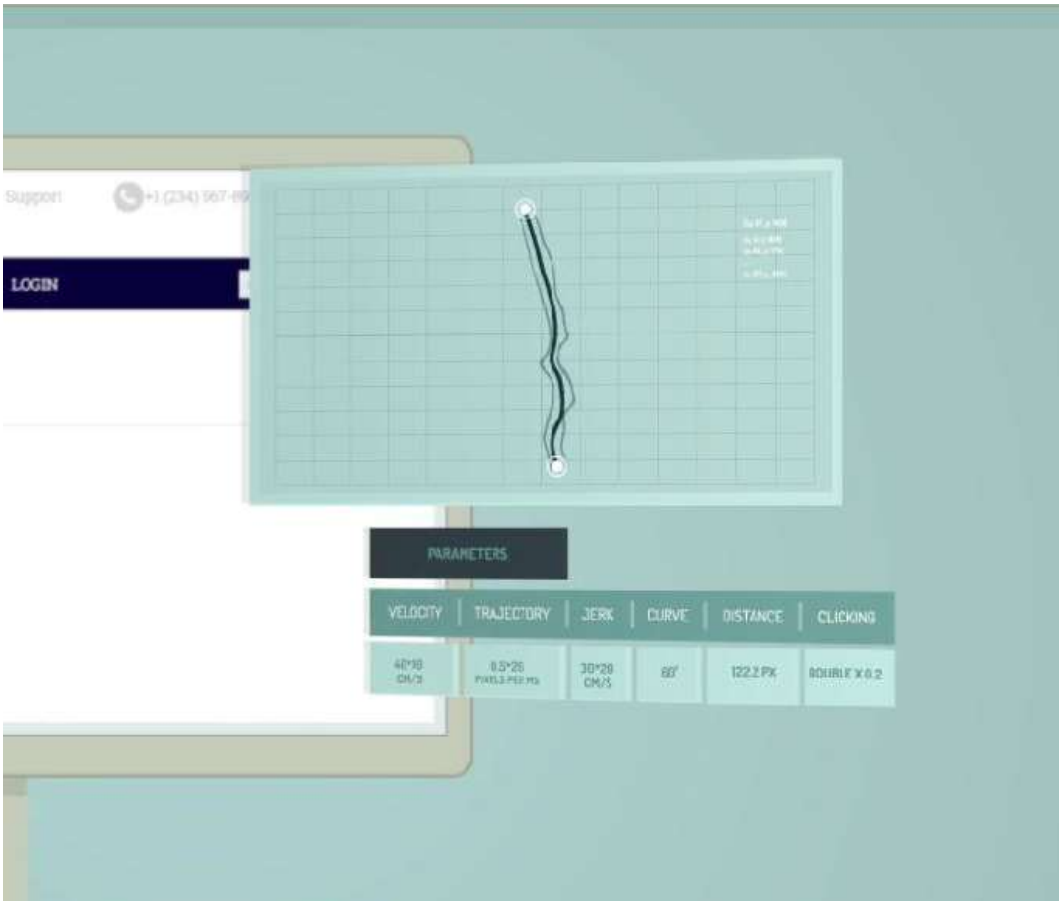

Bank-e-Moon
24/7 Support
ABOUT US
PRODUCTS
SERVICES
INVESTING
LOGIN
MEMBER LOGIN
Home | Member Login
USERNAME
hayonatan
PASSWORD
TOKEN
LOGIN
Forgot Password?
280.7 PX
320.5 PX
122.2 PX


LOGIN
PARAMETERS
VELOCITY
TRAJECTORY
JERK
CURVE
DISTANCE
CLICKING
122.2 PX

See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

204. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect estimates relative locations between text, input boxes, buttons, and advertisements as displayed by the client device by using, at least in part, a relative (as opposed to absolute) distance of 122.2 PX (pixels) that is a measure of the distance between the click selecting the username input box and the click selecting the password input box. Pixels are a relative distance measuring unit that is tied to the number of pixels contained in the rendered page (*e.g.*, 4K image rendering is 4096 pixels by 2160 pixels). It is a relative size because the absolute size depends on the absolute geometry of the display screen used in the client's device and the pixel shape.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4.

205. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, Trusteer Pinpoint Detect, the presentation information includes at least one of protocol information, formatting information, positional information, rendering information, style information, transmission encoding information, information describing how different layers of a style sheet are to be rendered by the client device, or information changing a definition of a function in a code library at the

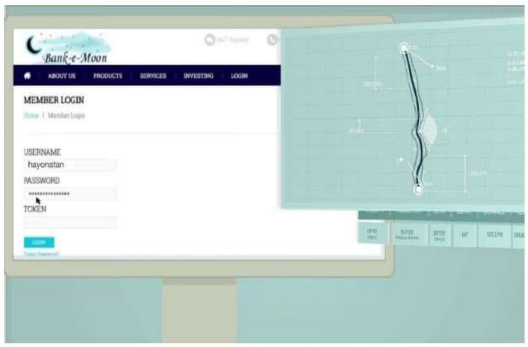
client device. For example, The Accused Products estimate locations of rendered page geometry of the features and functions by using, at least in part, a distance of 122.2 pixels that is derived by subtracting the pixel locations of the two mouse clicks that select the two input boxes (USERNAME and PASSWORD for example).

206. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the presentation information includes protocol information, for example, TCP/IP, UDP/IP, HTTP, or FTP.

207. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the Accused Products select presentation information that includes at least one of protocol information, formatting information, positional information, rendering information, style information, transmission encoding information, and information describing how different layers of a style sheet is to be rendered by the client.

208. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the Accused Products select presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed using JavaScript code in the client's web browser and the IBM Trusteer Mobile SDK, which information includes one or more of at least formatting information, positional information, rendering information, and style information.

209. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, the Accused Products attach mousemove event listener to the rendered page for the purposes of asking for clientX, clientY (i.e., the X,Y coordinates of the mouse click). The Accused Products attach mousedown mouseup click event listeners on the selected transactional fields - username and password. The event listener functions are re-polymorphed each session.



See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4

210. As shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in Trusteer Pinpoint Detect, the transactional information includes at least one of text, data, pictorial information, image information, information requested by the server to perform a service for the client device, authentication information, refinement information on a type of service requested by the client device, financial information, or data management information.

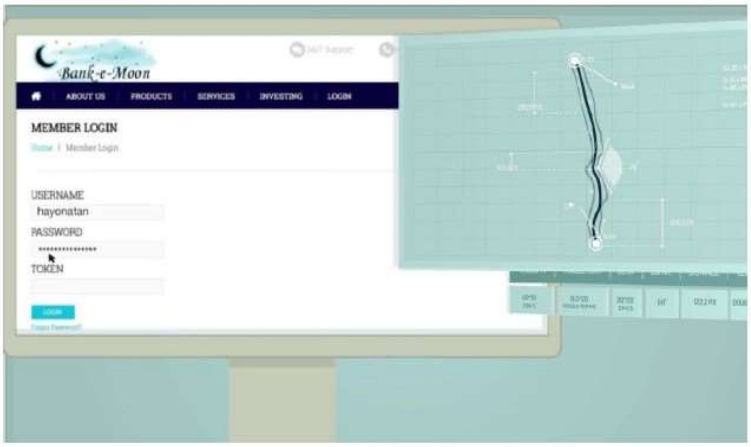
211. For example, as shown in the IBM Trusteer – Behavioral Biometrics Demo Video, in the Accused Products, the transactional information includes at least one of text, data, or pictorial information.

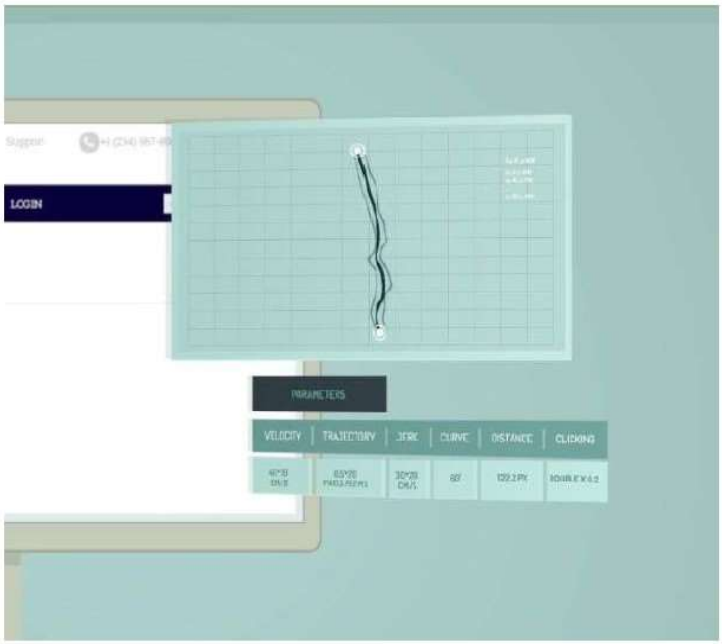
212. In the Accused Products the transactional information includes information requested by the server to perform a service for the client device.

213. In the Accused Products, a customer's server receives a request for the member login web page from the client device of an end user. In response to that request, the server selects transactional information, such as the "USERNAME," "PASSWORD," and "TOKEN" field titles and data entry boxes, to transmit from the server to the communicatively coupled client device to request the corresponding information from the end user of the client device.

214. The Accused Products estimate relative locations between text, input boxes, buttons, and advertisements as displayed by the client device by using, at least in part, a relative (as opposed to absolute) distance of 122.2 PX (pixels) that is a

measure of distance between the click selecting the username input box and the click selecting the password input box. Pixels are a relative distance measuring unit that is tied to the number of pixels contained in the rendered page (e.g., 4K image rendering is 4096 pixels by 2160 pixels). It is a relative size because the absolute size depends on the absolute geometry of the display screen used in the client's device and the pixel shape.





See IBM Trusteer – Behavioral Biometrics Demo Video, *available at* https://www.youtube.com/watch?v=kemFd5t2nD4

215. The Accused Products satisfy each and every element of each asserted claim of the '682 Patent either literally or under the doctrine of equivalents.

216. IBM's infringing activities are and have been without authority or license under the '682 Patent.

217. As a result of IBM's unlawful activities, SunStone has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, SunStone is entitled to preliminary and/or permanent injunctive relief.

218. IBM's infringement of the '682 Patent has injured and continues to injure SunStone in an amount to be proven at trial.

219. At least as early as July 2, 2016, Nick Coleman, IBM's Global Head Cyber Security Intelligence, requested a demonstration of SunStone's technology, as described in the '682 Patent.

220. SunStone is informed and believes that despite IBM's knowledge of the '682 Patent and SunStone's patented technology, IBM made the deliberate decision(s) to sell products and services that it knew infringe SunStone's '682 Patent.

221. SunStone is informed and believes that IBM has undertaken no efforts to avoid infringement of the '682 Patent, despite IBM's knowledge and understanding that IBM's products and services infringe these patents. Thus, IBM's infringement of '682 Patent is willful and egregious, warranting enhancement of damages.

222. As such, IBM has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '682 Patent, justifying an award to SunStone of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285. Pursuant to 35 U.S.C. § 154(d), SunStone provided notice of United States Patent Application Serial No. 16/298,537 to IBM on December 21, 2020, via its counsel on during a conference call and subsequent email communication. IBM had actual notice of the published patent application at least as early as December 21, 2020.

COUNT IV – INDUCED PATENT INFRINGEMENT OF THE '682 PATENT

223. SunStone realleges and incorporates by reference the allegations set forth above, as if set forth verbatim herein.

224. As set forth above, IBM is liable for indirect infringement under 35 U.S.C. § 271(b) of at least claims 1-11 and 21-29 of the '682 Patent at least as early as service of this Amended Complaint because it knowingly encourages, aids, and

directs others (*e.g.*, end users and customers) to use and operate the Accused Products in an infringing manner and to perform the claimed methods of the '682 Patent.

225. Since at least as early as December 21, 2020, IBM has had knowledge of United States Patent Application Serial No. 16/298,537. Since that time, IBM has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including IBM's customers, to use the Accused Products in a manner that infringe the '682 Patent. This is evident when IBM encourages and instructs customers and other end users in the use and operation of the Accused Products via advertisement, technical material, instructional material, and otherwise.

226. Since at least the service of this Amended Complaint, IBM has had knowledge of the '682 Patent. Since that time, IBM has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including IBM's customers, to use the Accused Products in a manner that infringe the '682 Patent. This is evident when IBM encourages and instructs customers and other end users in the use and operation of the Accused Products via advertisement, technical material, instructional material, and otherwise.

227. IBM specifically intends the Accused Products to be used and operated to infringe one or more claims, including at least claims 1-11 and 21-29, of the '682 Patent.

228. IBM encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

229. As detailed above, IBM has instructed its customers to use the accused methods and Accused Products in an infringing manner.

230. IBM had knowledge of the '537 Application at least as early as December 21, 2020.

231. IBM had actual notice of the published patent application at least as early as December 21, 2020.

232. IBM makes, uses, offers for sale, or sells in the United States the invention as claimed in the published patent application.

233. IBM's analysis and knowledge of the '537 Application combined with its ongoing activity demonstrates IBM's knowledge and intent that the identified features of its Accused Products be used to infringe the '682 Patent.

234. IBM's analysis and knowledge of the '682 Patent combined with its ongoing activity demonstrates IBM's knowledge and intent that the identified features of its Accused Products be used to infringe the '682 Patent.

235. IBM's knowledge of the '682 Patent and SunStone's infringement allegations against IBM combined with its knowledge of the Accused Products and how they are used to infringe the '682 Patent, consistent with IBM's promotions and instructions, demonstrate IBM's specific intent to induce PinPoint Detect and Trusteer Mobile users to infringe the '682 Patent.

236. SunStone is entitled to recover from IBM compensation in the form of monetary damages suffered as a result of IBM's infringement in an amount that cannot be less than a reasonable royalty together with interest and costs as fixed by this Court.

JURY DEMAND

237. SunStone hereby demands a trial by jury of all issues so triable pursuant to Fed. R. Civ. P. 38.

PRAYER FOR RELIEF

SunStone prays for the following relief:

(A) An entry of judgment that IBM has infringed and is directly infringing the '870 Patent and the '682 Patent;

(B) An entry of judgment that IBM has infringed and is indirectly infringing the '870 Patent and the '682 Patent;

(C) Judgment that the '870 Patent and the '682 Patent are valid and enforceable;

(D) A permanent injunction against IBM and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the '870 Patent and the '682 Patent and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

(E) An award to SunStone of such damages as it shall prove at trial against IBM that is adequate to fully compensate SunStone for IBM's infringement of the '870 Patent and the '682 Patent, said damages to be no less than a reasonable royalty;

(F) A determination that damages against IBM are available under 35 U.S.C. § 154(d);

(G) A determination that IBM's infringement has been willful, wanton, deliberate, and egregious;

(H) A determination that the damages against IBM be trebled or for any other basis within the Court's discretion pursuant to 35 U.S.C. § 284;

(I) A finding that this case against IBM is "exceptional" and an award to SunStone of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

(J) An accounting of all infringing sales and revenues of IBM, together with post judgment interest and prejudgment interest from the first date of infringement of the '870 Patent and the '682 Patent;

(K) Such further and other relief as the Court may deem proper and just.

Respectfully submitted this 26th day of March 2021.

By: */s/Christopher E. Hanba*

Christopher E. Hanba
State Bar No. 24121391
chris@connorkudlaclee.com
Kevin S. Kudlac
State Bar No. 00790089
kevin@connorkudlaclee.com
Jennifer Tatum Lee
State Bar No. 24046950
jennifer@connorkudlaclee.com
Cabrach J. Connor
State Bar No. 24036390
cab@connorkudlaclee.com
Joshua G. Jones
State Bar No. 24065517
josh@connorkudlaclee.com

CONNOR KUDLAC LEE PLLC
609 Castle Ridge Road, Suite 450
Austin, Texas 78746
512.777.1254 Telephone
888.387.1134 Facsimile

ATTORNEYS FOR PLAINTIFF SUNSTONE INFORMATION DEFENSE, INC.