

**IN THE UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF VIRGINIA**

SUNSTONE INFORMATION DEFENSE, INC.,)	
)	
<i>Plaintiff,</i>)	Civil Action No. _____
)	
v.)	
)	JURY TRIAL DEMAND
F5 NETWORKS, INC. and)	
CAPITAL ONE FINANCIAL)	
CORPORATION)	
)	
<i>Defendants.</i>)	
)	
_____)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff SunStone Information Defense, Inc. files this Complaint for Patent Infringement and Demand for Jury Trial against F5 Networks, Inc. and Capital One Financial Corporation for infringement of United States Patent Nos. 9,122,870 and 10,230,759.

Pursuant to 35 U.S.C. § 154 (d), SunStone provides notice of additional patent claims that have been published in connection with United States Patent Application Serial No. 16/298,537. SunStone has paid all required issue fees. Upon issuance, SunStone intends to amend this Complaint to assert forthcoming U.S. Patent No. 10,____,____ and seek pre-issuance damages pursuant to 35 U.S.C. § 154 (d).¹

¹ The precise patent number will be assigned by the United States Patent and Trademark Office upon notice of issuance.

THE PARTIES

1. Plaintiff SunStone (“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. F5 Networks, Inc. (“F5”) is a Washington corporation with its principal place of business at 801 5th Avenue, Seattle, Washington, 98104. F5 is registered to do business in Virginia and may be served through its agent for service of process CT Corporation at 4701 Cox Road, Suite 285, Glen Allen, Virginia, 23060. In January 2020, F5 acquired all right, title and interest in and to Shape Security, Inc. (“Shape”).

3. F5 maintains a regular and established place of business in this District through multiple permanent physical facilities, including 11911 Freedom Dr. #950, Reston, Virginia, 20190 and Two Discovery Square, 12012 Sunset Hills Road, Suite 900, Reston, Virginia, 20190.

4. Capital One Financial Corporation (“Capital One”) is a Virginia corporation with its principal place of business at 1680 Capital One Dr, McLean, Virginia, 22102.

5. Capital One is registered to do business in Virginia and may be served through its agent for service of process Corporation Service Company at 100 Shockoe Slip Fl. 2, Richmond, Virginia, 23219.

6. F5 regularly conducts and transacts business in Virginia, throughout the United States, and within the Eastern District of Virginia, and as set forth below, has committed and continues to commit, tortious acts of patent infringement within and outside of Virginia and within the Eastern District of Virginia. Further, F5 directly or indirectly uses, distributes, markets, sells, and/or offers to sell throughout the United States, including in this judicial district, various computer security products and services, including Shape Connect, ShapeShifter Elements, Shape

Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and Silverline Shape Defense, alone or in conjunction with one another (collectively, “the Accused Products”).

7. Capital One regularly conducts and transacts business in Virginia, throughout the United States, and within the Eastern District of Virginia, and as set forth below, has committed and continues to commit, tortious acts of patent infringement within and outside of Virginia and within the Eastern District of Virginia. Further, Capital One directly or indirectly uses throughout the United States, including in this judicial district, various computer security products and services, including at least one of the Accused Products.

JURISDICTION AND VENUE

8. This is an action for patent infringement arising under the patent laws of the United States, Title 35, United States Code, including 35 U.S.C. §§ 154, 271, 281, and 283-285.

9. This Court has exclusive subject matter jurisdiction over this case for patent infringement under 28 U.S.C. § § 1331 and 1338.

10. F5 is subject to the general and specific personal jurisdiction of this Court, based upon its regularly conducted business in the Commonwealth of Virginia and in the Eastern District of Virginia (“District”), including conduct giving rise to this action.

11. F5 has conducted and does conduct business within the Commonwealth of Virginia.

12. F5 maintains a regular and established place of business in this District through a permanent physical facility located at 11911 Freedom Dr. #950, Reston, Virginia 20190. Ex. 1, F5 Regional Offices, *available at* <https://www.f5.com/company/contact/regional-offices> (last visited Jan. 20, 2021); Ex. 2, F5 Federal Solutions, *available at* <https://www.f5.com/solutions/us-federal-government> (last visited Jan. 15, 2021).

13. F5 maintains another office for its F5 Government Solutions division at Two Discovery Square, 12012 Sunset Hills Road, Suite 900, Reston, Virginia, 20190.

14. F5, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), distributes, offers for sale, sells, and advertises (including the provision of an interactive web page) their products and/or services in the United States, the Commonwealth of Virginia, and the Eastern District of Virginia.

15. F5, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of their accused products and/or services, as described below, into the stream of commerce with the expectation that they will be purchased and used by consumers in the Eastern District of Virginia.

16. The accused products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Virginia.

17. F5 has committed acts of patent infringement within the Commonwealth of Virginia and, more particularly, within the Eastern District of Virginia.

18. Capital One is subject to the general and specific personal jurisdiction of this Court, based upon its regularly conducted business in the Commonwealth of Virginia and in the Eastern District of Virginia (“District”), including conduct giving rise to this action.

19. Capital One has conducted and does conduct business within the Commonwealth of Virginia.

20. Capital One maintains a regular and established place of business in this District through a permanent physical facility located at 11911 Freedom Dr. #950, Reston, Virginia 20190.

21. Capital One, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), distributes, offers for sale, sells, and advertises (including the

provision of an interactive web page) their products and/or services in the United States, the Commonwealth of Virginia, and the Eastern District of Virginia.

22. Capital One, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of their accused products and/or services, as described below, into the stream of commerce with the expectation that they will be purchased and used by consumers in the Eastern District of Virginia.

23. The accused products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Virginia.

24. Capital One has committed acts of patent infringement within the Commonwealth of Virginia and, more particularly, within the Eastern District of Virginia.

25. With respect to F5, venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 and 1400(b). F5 has transacted business in this District, and has directly committed acts of patent infringement in this District, and has a regular and established place of business in this District. F5 maintains several regular and established places of business in this District described above. SunStone is informed and believes that F5 employs a number of personnel in this District, including personnel involved in F5's infringement by and through at least the testing, demonstration, support, use, offer for sale, and sale of the accused products and services within Virginia.

26. With respect to Capital One, venue is proper in the Eastern District of Virginia under 28 U.S.C. §§ 1391 and 1400(b). Capital One resides in the Eastern District of Virginia. Capital One is incorporated in Virginia, headquartered in the Eastern District of Virginia, and maintains several regular and established places of business in this District as described above.

RELATIONSHIP TO THE EASTERN DISTRICT OF VIRGINIA

27. SunStone's technology has attracted interest from a variety of parties in various industries such as banking, hospitals, and the United States government, all within the subpoena power of the Eastern District of Virginia.

28. SunStone has leveraged its contacts with the United States government since at least 2012. For example, SunStone has had meetings, given presentations, and demonstrated its products and services at the Office of the Director of National Intelligence, National Security Agency, Defense Information Systems Agency, Department of Homeland Security, and United States Secret Service.

29. SunStone has also had discussions with other third parties via telephone, in-person, and over video conferences, including Leidos Holdings Inc., formerly known as Science Applications International Corporation (SAIC), which is based in Reston, Virginia.

30. In SunStone's efforts to leverage its contacts in Virginia, Maryland, and Washington, D.C., SunStone was informed on numerous occasions of F5 and Shape's efforts to sell the Accused Products. Often times, SunStone was informed by third parties of the similarities of the Shape product to the SunStone solution. Shape is now owned by F5.

31. In 2013, the NSA contracted with SunStone for use of SunStone's products and services. The SunStone implementation at the NSA is the commercial embodiment of the Asserted Patents. The SunStone implementation at the NSA and relevant witnesses regarding SunStone's NSA contract are located within the subpoena power of this District. SunStone further believes that other witnesses with relevant information are located within this District and/or within the subpoena power of this District.

32. F5 has a long history of conducting business in the Eastern District of Virginia. Several third parties in this District have information relevant to SunStone's claims.

33. For example, F5 contracts with Carahsoft Technology Corp. ("Carahsoft"), based in Reston, Virginia, as a reseller of F5 products and services, including the Accused Products. Carahsoft's training experience, purchase of the Accused Products, and implementation of the Accused Products, are relevant to SunStone's claims of patent infringement. According to Carahsoft:

Carahsoft Technology Corp. has been pleased to support F5 Networks in the public sector for nearly 10 years. Today, Carahsoft helps to conduct 95% of F5 Networks' federal business and was recently named F5's Federal Partner of the Year in 2018. Our extensive capabilities in sales, marketing, and renewal support have continued to generate demand and elevate F5's federal business since the inception of our partnership in 2010. A healthy and productive collaboration with F5's value-added reseller community has been vital to our success. We help this community align with F5's latest solutions, sales plays, use cases, and any updates to position F5 in the most effective way possible within the public sector.

Ex. 3, F5 Networks Carahsoft, *available at* <https://www.carahsoft.com/f5-networks#partners> (last visited Jan. 15, 2021).

34. F5 has developed the "Find a Unity+ Partner" program, which includes at last thirteen resellers in this District with information likely relevant to SunStone's claims. According to F5:

F5's UNITY Partner Program includes regional and global partners that build and deliver best-in-class IT solutions for customers of all sizes.

As an F5 UNITY Partner, participating companies have invested in networking, security, cloud, application development and deployment to help our clients solve the most complex application delivery challenges.

Ex. 4, Find a Unity+ Partner, *available at* <https://www.f5.com/partners/find-a-partner?partnerLocation=United%20States%3AVirginia&partnerPage=1> (last visited Jan. 15, 2021).

35. Several third parties located in the District incorporate F5 technology that is relevant to SunStone's claims. For example, a search of current job openings in Virginia shows that numerous companies implement F5 technology relevant to SunStone's claims. *See, e.g.*, Ex. 5 at 1, Job Opening at Scientific Research Corporation in Quantico, Virginia for Senior F5 WAF Network Engineer; Ex. 5 at 3, Job Opening at The Buffalo Group, LLC in Fort Belvoir, Virginia – Senior F5 System Engineer; Ex. 5 at 7, Job Opening at ManTech in Chantilly, Virginia for Cyber Security Engineer (F5); Ex. 5 at 12, Job Opening at Agile Defense, Inc. in Quantico, Virginia for Systems Engineer F5; Ex. 5 at 16, Job Opening at GuidePoint Security in Chantilly, Virginia for 5 Engineer; Ex. 5 at pg. 19, Job Opening at Leidos in Ashburn, Virginia for Senior Network Engineer (F5 firewall, F5 Big IP); Ex. 5 at 21, Job Opening at SkyePoint Decisions, Inc. in Sterling, Virginia and Springfield, Virginia for F5 Network Engineer; Ex. 5 at 23, Job Opening at NCI Information Systems Inc. in Radford, Virginia for Network Administrator Proxy/Load Balancer Focused on F5; Ex. 5 at 29, Job Opening at Proksi Systems in Reston, Virginia for Systems Engineer F5; Ex. 5 at 32, Job Opening at General Dynamics Information Technology in Fort Belvoir, Virginia for Sr. Network Engineer; Ex. 5 at 37, Job Opening at Comtech LLC in Reston, Virginia for F5 Engineer REMOTE; Ex. 5 at 39, Job Opening at Strategic Business Systems, Inc. in Springfield, Virginia for Network Engineer, F5 Professional; Ex. 5 at 41, Job Opening at Scientific Research Corporation in Quantico, Virginia for Senior F5 Waf Network Engineer Virtual; Ex. 5 at 46, Job Opening at SkyePoint Decisions, Inc. for F5 Network Engineer in Springfield, Virginia; Ex. 5 at 5, Job Opening at Bank of America in Richmond, Virginia for Network Services Engineer - F5 / Cisco; Ex. 5 at 53, Job Opening at MatchPoint Solutions in Reston, Virginia for F5 Network Engineer; Ex. 5 p. 55, Job Opening at General Dynamics Information Technology in Fort Belvoir, Virginia for Sr. Network Engineer; Ex. 5 at 58, Job

Opening at Apertus Partners in Reston, Virginia for F5 Engineer; Ex. 5 at 60, Job Opening at Jobot in Springfield, Virginia for F5 Engineer.

36. Similarly, Capital One is headquartered in McLean, Virginia. Capital One also has corporate offices in Richmond, Virginia. Capital One is a customer of F5 and, as described below, infringes the Asserted Patents. According to F5:

In many open banking applications, every millisecond matters. With F5, you can achieve previously impossible speeds through real-time APIs. Take Capital One's developer portal. F5 technology has enabled them to scale applications to 12 billion operations per day, with peaks of 2 million operations per second at latencies of just 10–30 milliseconds.

Ex. 6, Open Banking, *available at* <https://www.f5.com/solutions/banking-and-financial-services/open-banking> (last visited Jan. 15, 2021).

37. In 2015, SunStone began discussions with Capital One. During discussions, SunStone spoke with and presented detailed information to Capital One by demonstrating the SunStone technology to numerous individuals at Capital One, including the key decisionmakers Tony Spinelli and Erik Rolf.

38. Tony Spinelli was formerly the Senior Vice President, Chief Information Security Officer (CISO) of Information Security and Risk Management for Capital One. Mr. Spinelli currently lives and works in the Washington, D.C. area. Ex. 7, LinkedIn Profile, *available at* <https://www.linkedin.com/in/tspinelli/> (last visited Jan. 15, 2021).

39. Erik Rolf is currently the Director of Cloud Security Architecture working at Capital One in McLean, Virginia. Ex. 8, LinkedIn Profile, *available at* <https://www.linkedin.com/in/rolferik/> (last visited Jan. 15, 2021).

40. Numerous third parties in the District have discoverable information relevant to SunStone's claims.

SUNSTONE'S INNOVATIONS

41. SunStone was founded in 2011 by Dr. David Ford and is still in business.

42. 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.

43. 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.

44. SunStone is a cybersecurity provider that offers several products for the rapidly developing cyberthreat prevention market, including mobile and desktop solutions. 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.

45. SunStone has been awarded, and continues to prosecute, numerous patents covering innovations in the United States and around the world resulting directly from SunStone’s research and development efforts.

46. SunStone designed software and technology for network security using these patented technologies.

47. 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. 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.

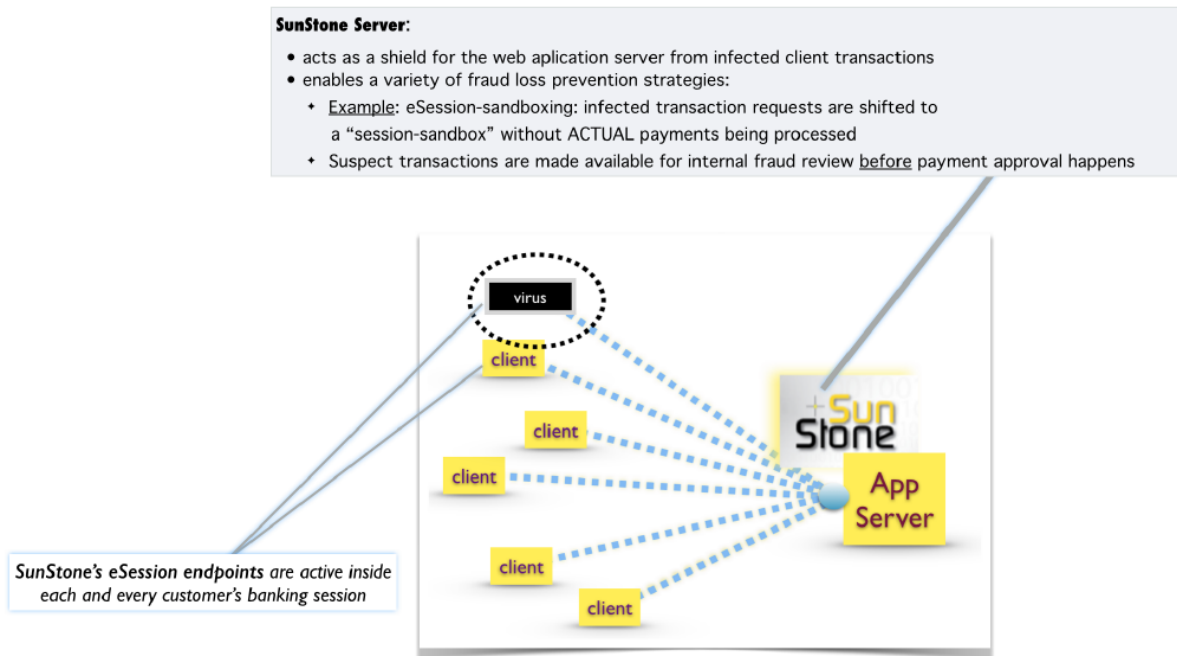
48. SunStone does not offer two-factor authentication. Instead, it offers a much more elaborate and protective service that detects, prevents, and deters cyber-criminals before they achieve their purpose.

49. 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 valuable. 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.

50. 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.

51. As an attack tool used by hackers and virus manufacturers, the virus polymorphism technique is employed to successfully blast its way 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.

52. 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 browser download and installation is required.



53. 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.

54. 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.

55. Beginning in the early to mid-2000s, financial trojan 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.

56. 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.

57. 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 within the subpoena power of this District.

58. In 2013, the NSA contracted with SunStone for use of SunStone’s products and services. The SunStone implementation at the NSA is the commercial embodiment of the Asserted Patents. The SunStone implementation at the NSA and relevant NSA witnesses regarding SunStone’s contract with the NSA are located within the subpoena power of this District. SunStone further believes that witnesses with relevant information are located within this District and/or within the subpoena power of this District.

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

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

SUNSTONE’S TECHNOLOGY

61. SunStone’s patents are seminal patents in the field of cybersecurity directed against virus polymorphism.

62. 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.

63. 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.

64. 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.

65. 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 (0,1), (1,2), (2,3), (3,4), etc. From an engineering perspective, a GUI is 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 to the pixels must not remain fixed or static.

66. 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.

67. 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.

SUNSTONE'S ASSERTED PATENTS

UNITED STATES PATENT NO. 9,122,870

68. On September 1, 2015, the United States Patent and Trademark Office duly and legally issued United States Patent No. 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. The '870 Patent 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. A true and correct copy of the '870 Patent is attached hereto as Exhibit 9.

69. SunStone is the owner by assignment from the inventor, David Ford, of all right, title, and interest in and to the '870 Patent.

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

71. The '870 Patent 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 Patent Office issued the '870 Patent on September 1, 2015, after a full and fair examination.

73. As the owner of the '870 Patent, SunStone holds all substantial rights in and to the '870 Patent, 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.

74. 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.

75. The '870 Patent is cited on the face of numerous patents by SunStone's competitors.

76. The '870 patent is cited on the face of U.S. Patent No. 9,411,958 B2, which is assigned to Shape.

77. The '870 Patent describes a method for validating communications in an open architecture system.

78. The '870 Patent describes an apparatus for validating communications in an open architecture system.

79. Claim 39 of the '870 Patent recites:

A method comprising:

receiving, in a security server from a transaction server, transactional information to transmit to a client device based on a transaction with the client device;

receiving, in the security server from the transaction server, presentation information corresponding to the transactional information;

modifying, via the security server, at least some of the presentation information;

transmitting, via the security server, the modified presentation information and transactional information to the client device;

determining, via the security server, an acceptable response based on i) the modified presentation information and the transactional information, ii) how the client device is configured to render the transactional information, and iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device; and

responsive to information in a response message from the client device not matching the acceptable response, providing an indication there is a malicious application affecting communications between the transaction server and the client device, wherein the acceptable response 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.

80. 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.

81. 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.

82. 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.

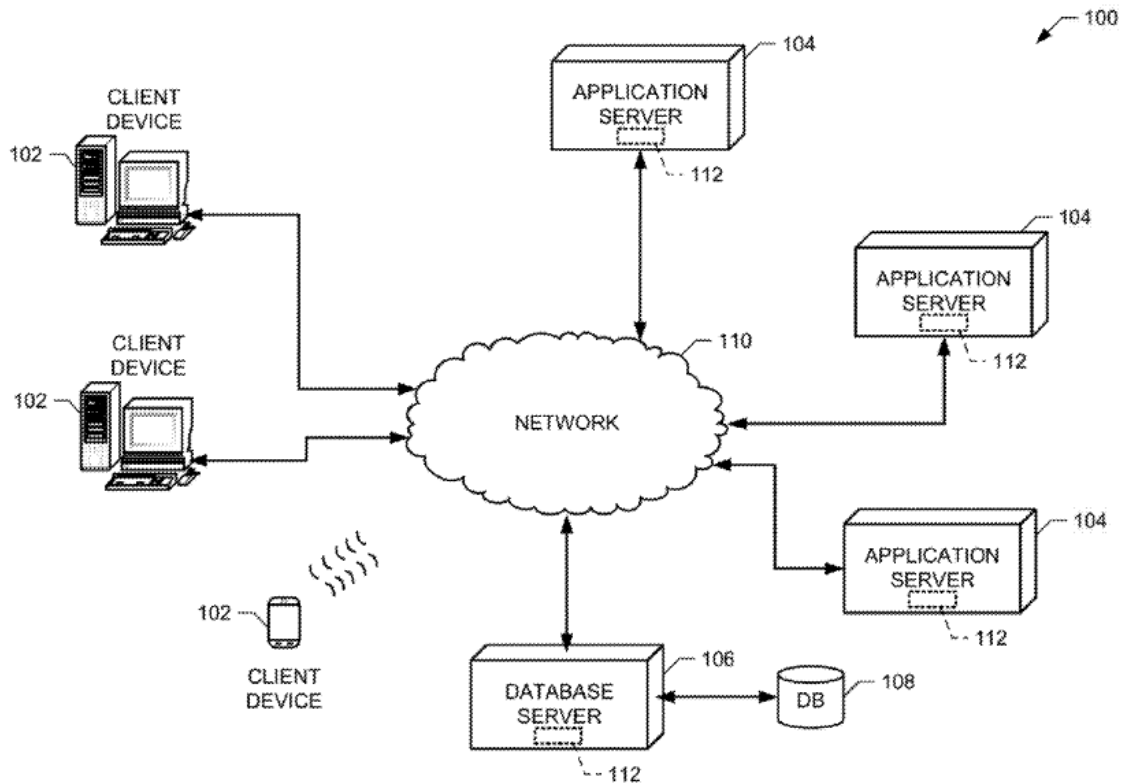


FIG. 1

'870 Patent at Fig. 1.

83. 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.

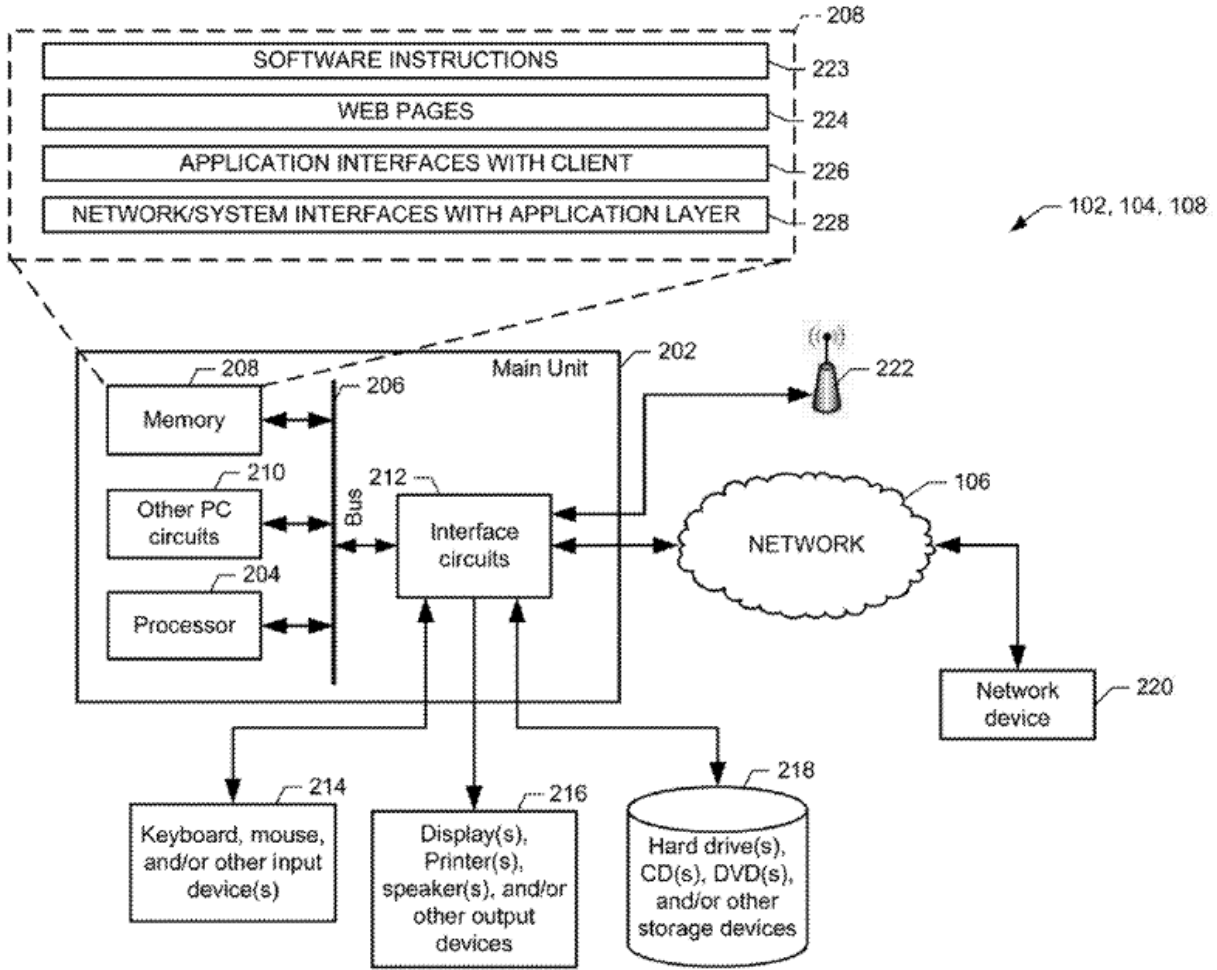
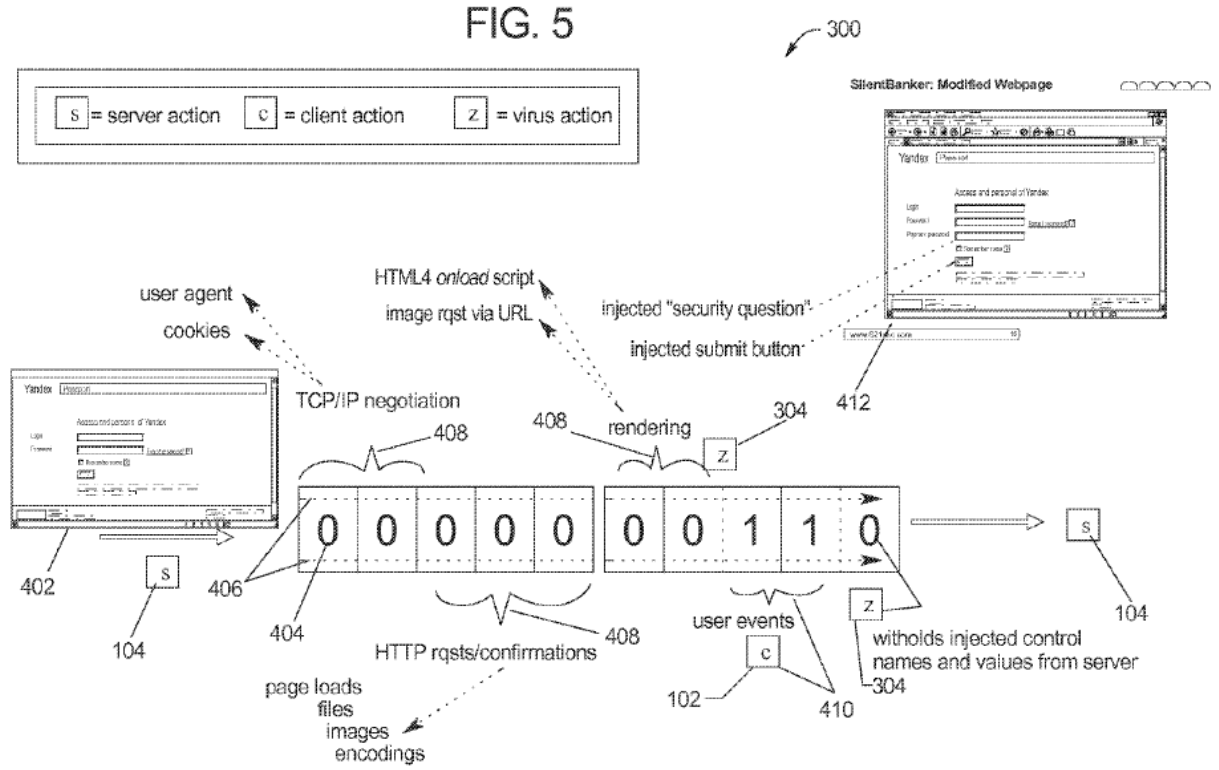


FIG. 2

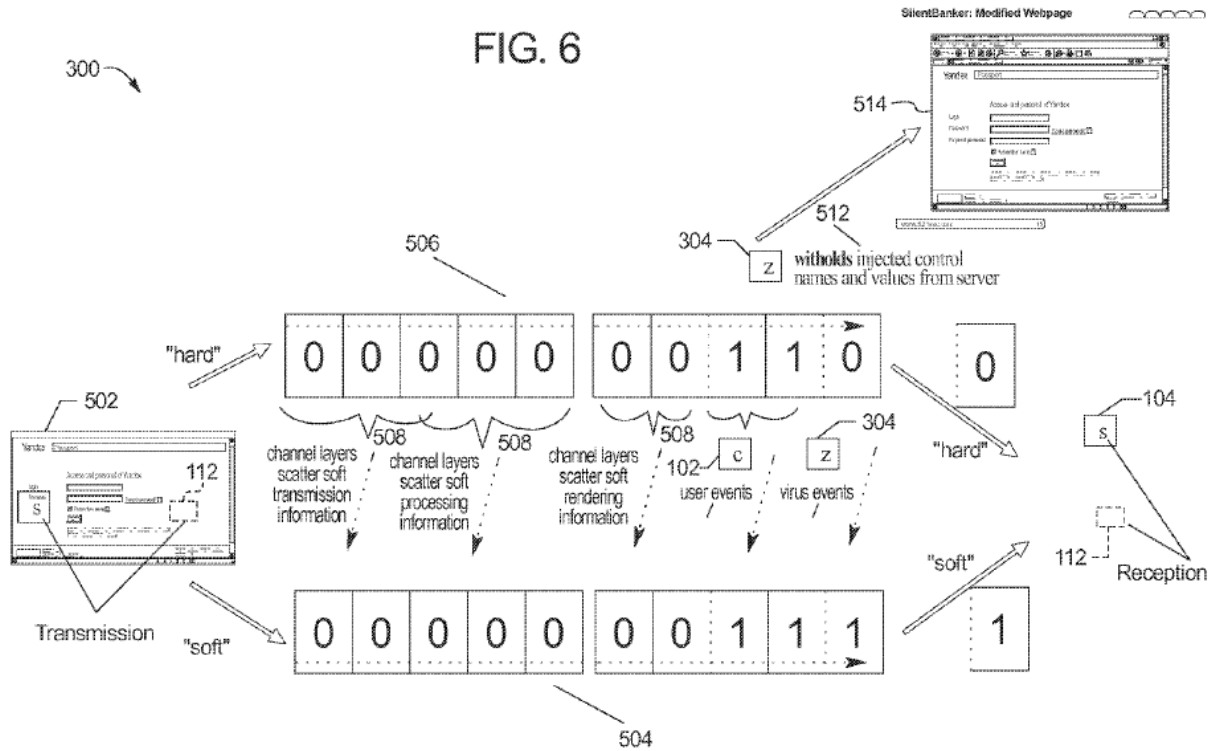
'870 Patent at Fig. 2.

84. 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.



'870 Patent at Fig. 5.



'870 Patent at Fig. 6.

85. At least Claims 1-20 and 37-38 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.

86. 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.

87. 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, nor routine.

88. 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, nor routine.

89. 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, nor routine.

90. 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, nor routine.

91. 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, nor routine.

92. 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, nor routine.

93. 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.

94. 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.

95. 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.

UNITED STATES PATENT NO. 10,230,759

96. On March 12, 2019, the United States Patent and Trademark Office duly and legally issued United States Patent No. 10,230,759 (the “759 Patent”), titled “Method 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. A true and correct copy of the '759 Patent is attached hereto as Exhibit 10.

97. SunStone is the owner by assignment from the inventor, David Ford, of all right, title, and interest in and to the '759 Patent.

98. The '759 Patent issued from U.S. Patent Application No. 14/841,083 filed on August 31, 2015.

99. The '759 Patent claims priority to United States Patent No. 9,122,870, filed September 20, 2012, which 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

100. The Patent Office issued the '759 Patent on March 12, 2019, after a full and fair examination.

101. As the owner of the '759 Patent, SunStone holds all substantial rights in and to the '759 Patent, including the right to exclude others from practicing its patented inventions, the right to enforce the '759 Patent, and the right to sue and recover damages for infringement of the '759 Patent.

102. The '759 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.

103. The '759 Patent is cited on the face of numerous patents by SunStone's competitors.

104. The '759 patent is cited on the face of U.S. Patent No. 9,411,958 B2, which is assigned to Shape, which was acquired by F5 in January 2020.

105. The '759 Patent describes a method for validating communications in an open architecture system.

106. Claim 15 of the '759 Patent recites:

An apparatus comprising:

a security processor configured to:

receive, from a transaction server, i) hard information to transmit to a client device related to a transaction with the client device, the hard information including at least one of a) a data field in a webpage for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage that provides information related to the transaction, and ii) soft information including a first set of program code for the webpage that specifies how the hard information is to be displayed on the client device;

determine a variation of the soft information configured to prevent a malicious application from identifying the transaction with the client device, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed on the client device;

responsive to determining the variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the second set of program code;

responsive to determining that the variation of the soft information changes how the hard information is displayed, determine a second variation of the soft information configured to prevent a malicious application from identifying the transaction with the client device, the second variation of the soft information including a third set of program code that specifies how the hard information is to be displayed on the client device;

responsive to determining the second variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the third set of program code; and transmit at least one message to the client device including the hard information and the variation of the soft information or the second variation of the soft information.

107. The '759 Patent describes a method and apparatus for determining a variation of soft information configured to prevent a malicious application from interacting with hard information and determining the variation of the soft information does not change how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information.

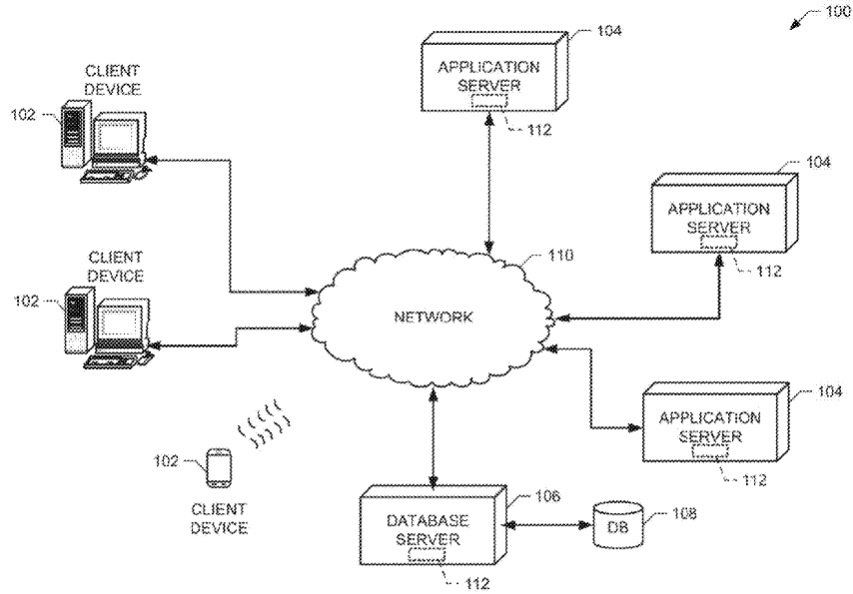


FIG. 1

108. Mr. Ford, the inventor of the '759 Patent, recognized that “[c]onventional 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.” ’759 Patent 2:40-44. Therefore, by using variations of soft information (which specifies how hard information is to be rendered and displayed by a client device) to specify how hard information (data, text, and other information that is important for carrying out a transaction by a client) managed by a server is displayed on a client device, the security processor can create a prediction as to how the client device will render the hard information and then compare the information received from the client device to determine if a malicious application has affected or otherwise altered communications between the server and client device.

109. The '759 Patent greatly improved upon the prior art at least because malicious applications are specifically configured to identify valid codewords and switch between such valid codewords. As a result, traditional error correction schemes cannot detect the switch because they

have no way of identifying whether an error has occurred. A traditional communication system would view the resulting altered codeword as valid from its point of view.

110. The '759 Patent describes and claims a specific way to overcome the problem of detecting malicious applications by using variations in soft information to form a best guess as to how hard information is displayed by a client device, comparing a response from the client device to the prediction, and then, if the information included in the response does not match, or is not close enough to the prediction, then it will be determined that a malicious program is effecting the communication system and a failsafe procedure can then be implemented.

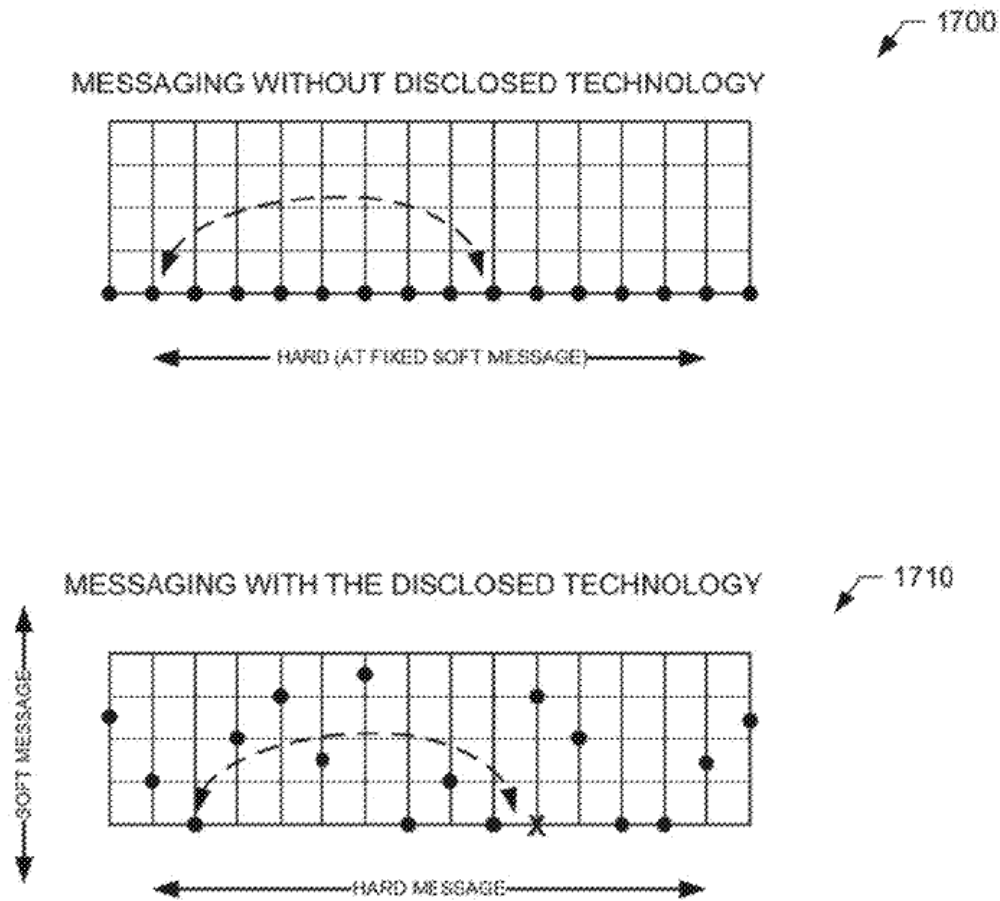


FIG. 17

111. A person of ordinary skill in the art at the time of the invention would have recognized that the steps (and combination of steps) and methods claimed in the '759 Patent were, at the time of invention, unconventional and describe a method and apparatus for malicious application detection that, at the time of the invention, was not routine.

112. A person skilled in the art at the time of the invention would have understood that receiving from a transaction server “i) hard information to transmit to a client device within at least one message related to a transaction with the client device, the hard information including at least

one of a) a data entry field in a webpage for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage that provides information related to the transaction, and ii) soft information for transmission to the client device within the at least one message, the soft information including a first set of program code for the webpage that specifies how the hard information is to be displayed within the webpage on the client device” was not, at the time of the invention, conventional, well-understood, nor routine.

113. A person of ordinary skill in the art at the time of the invention would have understood creating “a variation of the soft information configured to prevent a malicious application from determining the transaction with the client device by interacting with the hard information, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed within the webpage on the client device” was not, at the time of the invention, conventional, well-understood, nor routine.

114. A person of ordinary skill in the art at the time of the invention would have understood that determining “whether the variation of the soft information changes how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information” was not, at the time of the invention, conventional, well-understood, nor routine.

115. A person of ordinary skill in the art at the time of the invention would have understood that having determined that the variation of soft information does not change how the hard information is displayed and then replacing “the first set of program code with the second set of program code for the at least one message and transmit[ting] the at least one message to the client device including the hard information and the variation of the soft information” was not, at the time of the invention, conventional, well-understood, nor routine.

116. A person of ordinary skill in the art at the time of the invention would have understood that having determined that “the variation of the soft information changes how the hard information is displayed at the client device, [and having determined that] a second variation of the soft information configured to prevent a malicious application from interacting with the hard information, the second variation of the soft information including a third set of program code that specifies how the hard information is to be displayed within the webpage on the client device” was not, at the time of the invention, conventional, well-understood, nor routine.

117. A person of ordinary skill in the art at the time of the invention would have understood that determining “the second variation of the soft information does not change how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information” was not, at the time of the invention, conventional, well-understood, nor routine.

118. A person of ordinary skill in the art at the time of the invention would have understood that having the response to “determining the second variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the third set of program code for the at least one message and transmit[ing] the at least one message to the client device including the hard information and the second variation of the soft information” was not, at the time of the invention, conventional, well-understood, nor routine.

119. A person of ordinary skill in the art at the time of the invention would have understood that the combination of steps in claim 1 of the '759 Patent was not, at the time of the invention, conventional, well-understood, or routine.

120. A person skilled in the art at the time of the invention would have understood that the claims of the '759 Patent recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of a security processor apparatus.

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

122. The novel use and arrangement of the specific combinations and steps recited in the '759 claims were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

UNITED STATES PATENT APPLICATION SERIAL NO. 16/298,537

123. SunStone filed United States Patent Application Serial No. 16/298,537 (the "'537 Application"), on March 11, 2019, and it 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. A true and correct copy of the Notice of Allowance, with final claims as amended and allowed, of the '537 Application is attached hereto as Exhibit 11.

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

125. Since February 6, 2020, all papers in the '537 Application prosecution file have been available to the public.

126. 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.

127. On December 18, 2020, SunStone paid the issue fee.

128. The '537 Application will issue in a form substantially identical to the claims listed in Exhibit 11.

129. Amended Claim 13 of the '537 Application (final Claim 10 of the patent to issue) recites:

Claim [10]. 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 a label of the presentation information,

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.

130. SunStone is the owner by assignment from the inventor, David Ford, of all right, title, and interest in and to the '537 Application.

131. The '537 Application 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.

F5 NETWORKS AND SHAPE SECURITY

132. F5 specializes in application services and application delivery networking ("ADN"). F5 technologies focus on the delivery, security, performance, and availability of web applications, including the availability of computing, storage, and network resources.

133. Shape was founded in 2011 by Derek Smith, Justin Call, and Sumit Agarwal. Smith became CEO, Call became VP of R&D, Agarwal became Chief Operating Officer (COO), and Shuman Ghosemajumder the chief technology officer (CTO). Ray Rothrock, Ted Schlein, and Gaurav Garg were members of the Board of Directors.

134. According to Shape,

Shape's founders Derek Smith, Justin Call, and Sumit Agarwal launched the company to deal with a pattern of increasingly sophisticated attack types they had observed.

Specifically, what they saw in the work they did at the Pentagon and in the defense industry was that automation was increasingly used by cybercriminals to create fraud on applications which were otherwise secure from a traditional security standpoint. Sumit coined the term "credential stuffing" at the time to describe one of the most dangerous types of automated attacks, where usernames and passwords

from one data breach were being used to attempt to log in to completely unrelated websites.

Ex. 12, Interview with Shuman Ghosemajumder, CTO of Shape Security (June 20, 2019), *available at* <https://vator.tv/news/2019-06-20-interview-with-shuman-ghosemajumder-cto-of-shape-security>.

135. After a Series A funding round, in February 2014, the company raised \$40 million in Series C funding from Norwest Venture Partners, Sierra Ventures, and prior investors Kleiner Perkins Caufield & Byers, Venrock, Google Ventures, Tomorrow Ventures and Allegis Capital.

136. CNBC named Shape #23 on a list of 50 disruptor companies of 2014. *See* Ex. 13, 2014 CNBC's Disruptor 50 (June 17, 2014), *available at* <https://www.cnbc.com/2014/06/17/cnbc-disruptor-50.html> (last visited Jan. 15, 2021).

137. F5 acquired Shape in January 2020 for approximately \$1 billion. *See* Ex. 14, F5 to Acquire Shape Security, Transforming Application Security (Dec. 19, 2019), *available at* <https://www.f5.com/company/news/press-releases/f5-to-acquire-shape-security> (last visited Jan. 15, 2021); Ex. 15, F5 Completes Acquisition of Shape Security (Jan. 24, 2020), *available at* <https://www.f5.com/company/news/press-releases/f5-completes-acquisition-of-shape-security> (last visited Jan. 15, 2021); Ex. 16, Shape Officially Joins F5 to Defend Every App from Fraud and Abuse (Jan. 24, 2020), *available at* <https://blog.shapesecurity.com/2020/01/24/1486/> (last visited Jan. 15, 2021).

138. As describe in F5's Annual Report, Form 10-k for the fiscal year ended September 30, 2020:

On January 24, 2020, we completed the acquisition of Shape Security ("Shape"), a leader in online fraud and abuse prevention, adding protection against automated attacks, bots, and targeted fraud to F5's world-class portfolio of application delivery and security solutions. The acquisition delivers value to customers by combining F5's expertise in powering over half of the world's applications across multi-cloud

environments, with Shape's insight from mitigating one billion application attacks per day through sophisticated AI, cloud-based analytics, and anti-fraud technologies. Together, F5 and Shape represent an end-to-end application security solution, reducing infrastructure complexity, protecting our customers against losses from online fraud, reputational damage, and disruptions to critical online services.

Ex. 17, Annual Report, Form 10-K, at 3 (Certified Nov. 13, 2020).

139. F5 represented in its Annual Report that:

Our acquisition of Shape Security brings the leader in online fraud and abuse prevention, adding protection against automated attacks, bots, and targeted fraud, to F5's world-class portfolio of application security and delivery technologies. Together, F5 and Shape represent an end-to-end application security solution, reducing infrastructure complexity, protecting our customers against losses from online fraud, reputational damage, and disruptions to critical online services.

Id. at 4.

140. According to F5:

Shape invented the field of credential stuffing protection, an attack where cybercriminals use stolen passwords from third-party data breaches to take over other online accounts. In 2018, the company was ranked by Deloitte as the #1 fastest-growing company by revenue in Silicon Valley, and it currently protects the largest banks, airlines, retailers, and federal agencies in the world. In addition to credential stuffing attacks, its fraud and abuse prevention platform defends against other advanced attacks that bypass security and fraud controls.

Ex. 18, *Defending every application in a multi-cloud world*, available at <https://www.f5.com/products/security/shape-security> (last visited Jan. 15, 2021).

141. According to F5:

Together, F5 and Shape can help to ensure that the world's applications operate effectively and securely, end-to-end.

The acquisition brings together F5, a global leader in application delivery and services, and Shape Security, a global leader in application fraud and abuse protection.

Together, our combined solutions can save our customers billions of dollars currently lost to fraud and abuse, and prevent reputational damage and disruptions to critical online services.

F5 + Shape delivers end-to-end application security using the industry's most sophisticated AI/ML platform for application defense—one that already provides accurate and effective security outcomes at scale more than 1 billion times a day for some of the largest, most-attacked applications in the world.

Id.

142. F5 products, apps, and websites change their source code constantly to prevent automated attacks. F5's products protect web apps from bots and other automated attacks by delivering continuous protection, even when attackers retool. The managed service prevents sophisticated attacks including those on the OWASP Automated Threats to Web Applications list. *See How Silverline Shape Defense Works* (June 1, 2020), *available at* <https://www.youtube.com/watch?v=wJS5xDfyAs4> (last visited Jan. 15, 2021).

143. F5's products, which include legacy Shape products and F5 products incorporating Shape technology, aim to block online threats from bots, malware, and phishing attacks. In addition, F5'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 How Silverline Shape Defense Works* (June 1, 2020), *available at* <https://www.youtube.com/watch?v=wJS5xDfyAs4> (last visited Jan. 15, 2021).

144. According to Shape, Shape's technology platform stops sophisticated fraud and cybercriminal attacks which bypass standard security controls. Ex. 12, Interview with Shuman Ghosemajumder, CTO of Shape Security (June 20, 2019), *available at* <https://vator.tv/news/2019-06-20-interview-with-shuman-ghosemajumder-cto-of-shape-security> (last visited Jan. 15, 2021).

145. Shape's annual revenue, when it was acquired by F5 in 2020, was approximately \$70 million. Ex. 19, F5 Networks will acquire Shape Security for \$1 billion to bolster online fraud protection services (Dec. 19, 2019), *available at* <https://www.geekwire.com/2019/f5-networks->

will-acquire-shape-security-1b-bolster-online-fraud-protection-services/ (last visited Jan. 15, 2021).

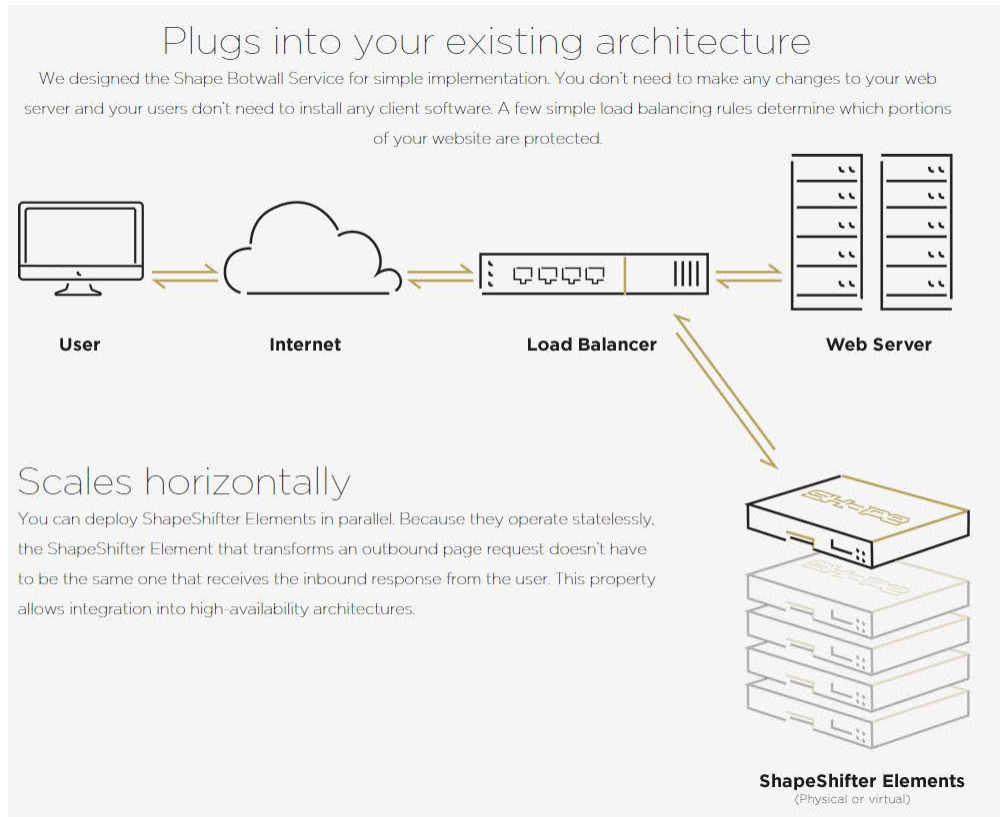
THE ACCUSED F5 PRODUCTS

146. According to F5, F5 offers a suite of application security and fraud prevention solutions that protect more than 4 billion transactions per week from attack. Ex. 18, Defending every application in a multi-cloud world, *available at* <https://www.f5.com/products/security/shape-security> (last visited Jan. 15, 2021).

147. F5 integrated Shape's products and services into F5's past and current offerings, including at least Shape Connect, ShapeShifter Elements, Shape Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and F5 Silverline Shape Defense.

148. According to F5, Shape Connect brings the Shape anti-bot and fraud protection technology to the mid-market at an affordable price. Ex. 20, New Solution from Shape Security brings Enterprise-grade Online Fraud Protection to the Mid-Market (May 7, 2019), *available at* <https://www.shapesecurity.com/press-releases/press-release-may2019> (last visited Jan. 15, 2021). Shape Connect allows organizations without security and IT teams to protect their online businesses against sophisticated bots, credential stuffing and other attacks that lead to fraud. *Id.*

149. According to F5, ShapeShifter Elements performs a method that defeats automated attacks on a website. ShapeShifter Elements implements a Bot Wall that works in conjunction with a load balancer to transform portions of webpage code to make a webpage undecipherable by an automated bot attack. Ex. 21, Introducing the Shape Shifter (Jan. 21, 2014), *available at* <https://blog.shapesecurity.com/tag/shape-shifter/> (last visited Jan. 15, 2021).



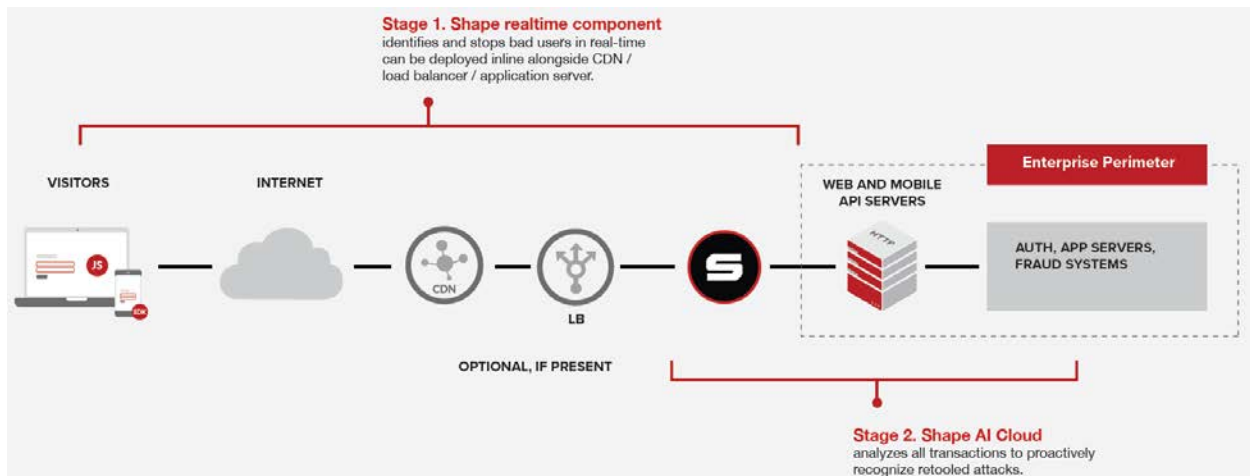
An example countermeasure: reference polymorphism

How do you change the very nature of HTML, to introduce a new security model, while still delivering open markup code to web browsers? Shape transforms pages in real-time to introduce polymorphic code which presents barriers which are difficult or impossible for attackers to overcome. Here's one simple example of code before and after being protected by the Shape Botwall Service:

ORIGINAL WEBSITE CODE (BEFORE)	TRANSFORMED WEBSITE CODE (AFTER)
<pre><form action="login_form.php"> <input id="username" name="username"/> <input id="password" name="password"/> <input type="submit"/> </form></pre> <p style="text-align: right;">Simplified HTML</p>	<pre><form action="R6bYEc2taB4e"> <input id="bNoeTn2bjf2F" name="p5Tb6SGCf63g"/> <input id="k5KbSjCT6p4t" name="yWTg3L082t2f"/> <input type="submit"/> </form></pre>

Ex. 22, The Shape Botwall Service, available at <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

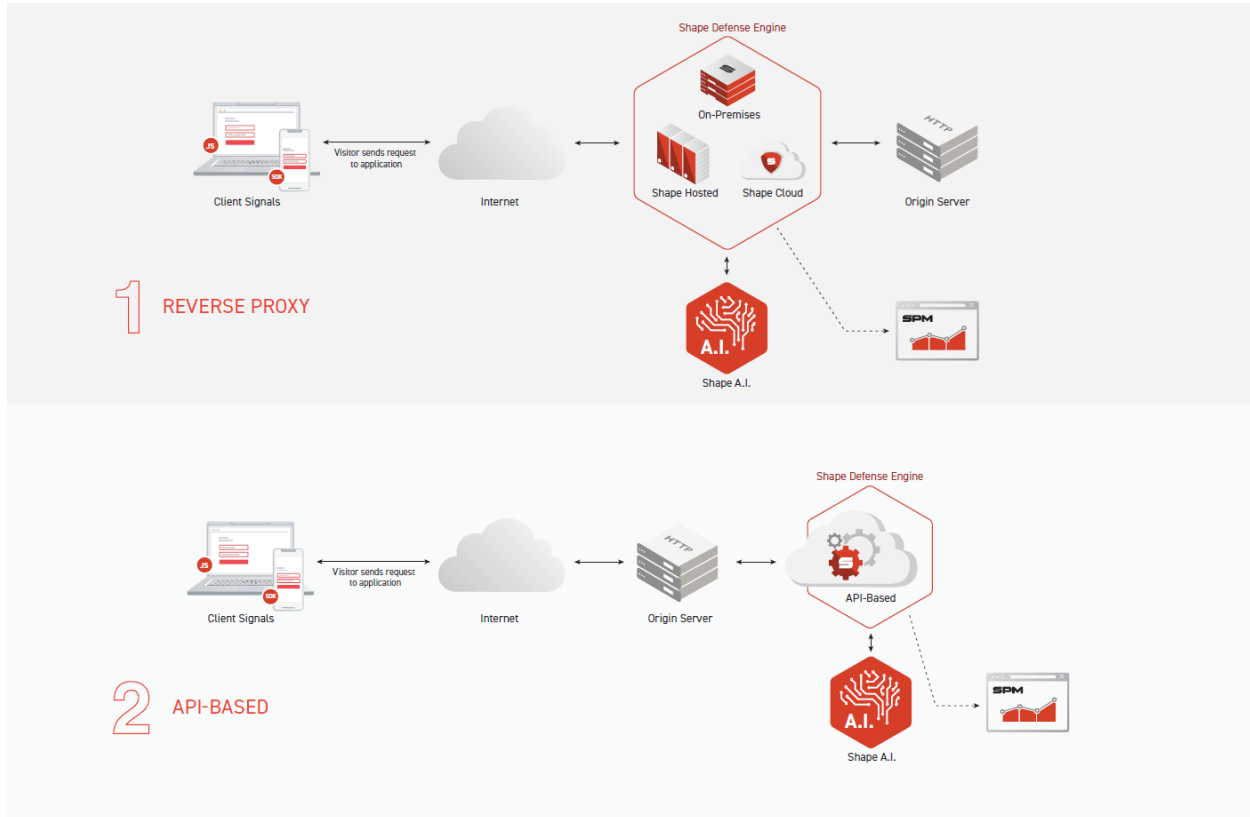
150. According to F5, Shape Defense uses a two-stage process to deliver highly accurate real-time detection and mitigation, as well as provide sustained protection through attacker retooling. *See* Ex. 23, 2020 Shape Defense Datasheet, <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021). Stage 1 evaluates each transaction across a set of proprietary risk factors that include network, activity, user, device and account factors. *Id.* These risk factors are evaluated in light of everything Shape has learned across its global customer base. *Id.* Shape Defense’s Stage 1 sees all traffic - including mitigated automation traffic – and also includes insights learned from detecting fraudulent activity across other Shape clients (aggregated defense from aggregated insights). *Id.* Shape Defense’s Stage 2 defense counters the attackers’ evolution with an after-action machine learning and human analysis. Specifically, Shape Defense’s Stage 2 defensive system leverages three tiers of supervised and unsupervised learning and provides unparalleled protection. Shape AI Cloud, which is integrated into Shape Defense, analyzes all transactions to proactively recognize retooled attacks.



Ex. 23, 2020 Shape Defense Datasheet, <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021);

Ex. 24, Shape Defense, *available at* <https://www.shapesecurity.com/shape-defense> (last visited Jan. 15, 2021).

151. According to F5, Shape Enterprise Defense determines in real-time if an application request is from a fraudulent source and then takes an enterprise-specified action, such as blocking, redirecting, or flagging the request. Ex. 25, Shape Security, *available at* <https://www.shapesecurity.com> (last visited Jan. 15, 2021); Ex. 26, Shape Enterprise Defense (last visited Dec. 30, 2020), *available at* <https://www.shapesecurity.com/shape-enterprise-defense> (last visited Jan. 15, 2021); Ex. 28, Shape Enterprise Defense Solution Overview (last visited Dec. 30, 2020), *available at* <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Enterprise%20Defense%20Solution%20Overview.pdf> (last visited Jan. 15, 2021);. The Shape Enterprise Defense product is used by eight of the top 12 US banks, five of the top ten global airlines, two of the top five global hotels, and two of the largest US government agencies. *See* Ex. 27, New Product Protects SMBs From Credential Stuffing Attacks (May 8, 2019), *available at* <https://www.securityweek.com/new-product-protects-smbs-credential-stuffing-attacks> (last visited Jan. 15, 2021).

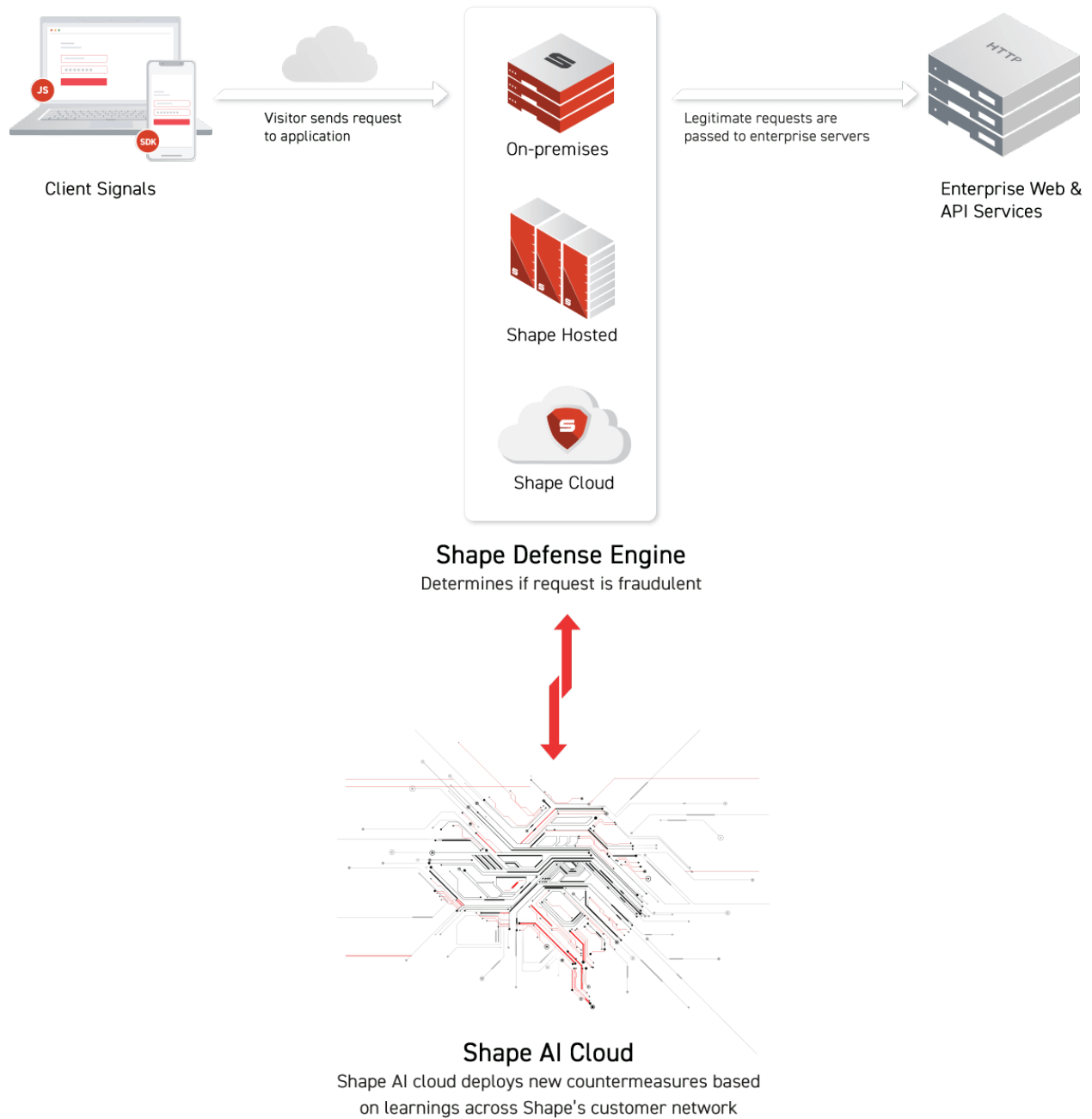


Ex. 28, Shape Enterprise Defense Solution Overview, available at

[https://info.shapesecurity.com/rs/935-ZAM-](https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Enterprise%20Defense%20Solution%20Overview.pdf)

[778/images/Shape%20Enterprise%20Defense%20Solution%20Overview.pdf](https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Enterprise%20Defense%20Solution%20Overview.pdf) (last visited Jan. 15, 2021).

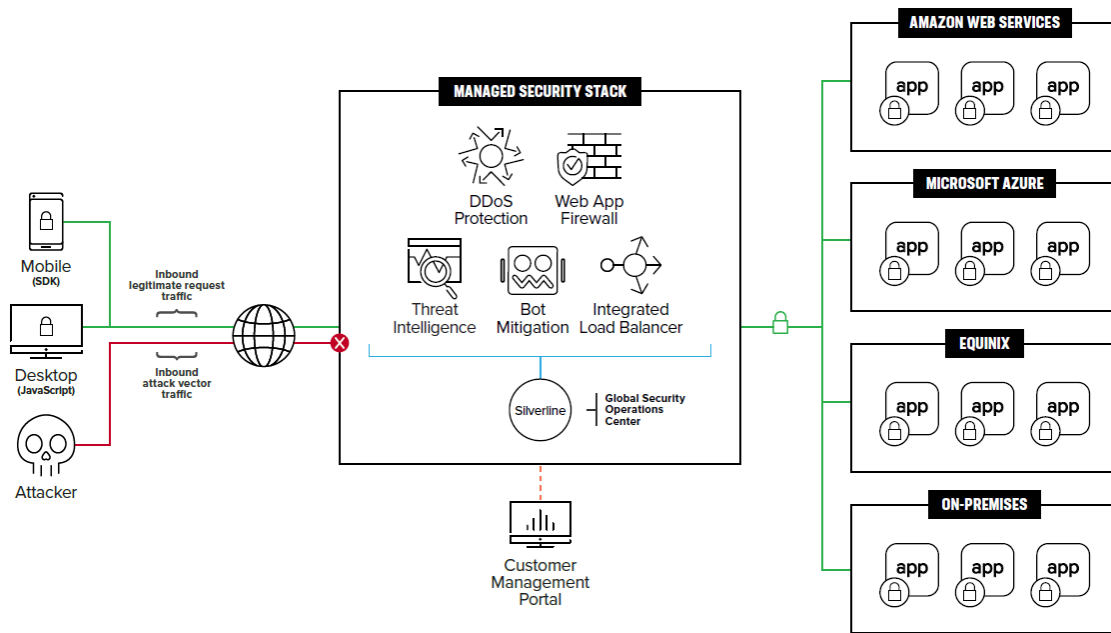
152. Shape Enterprise Defense uses the Shape Defense Engine in conjunction with the Shape AI Cloud.



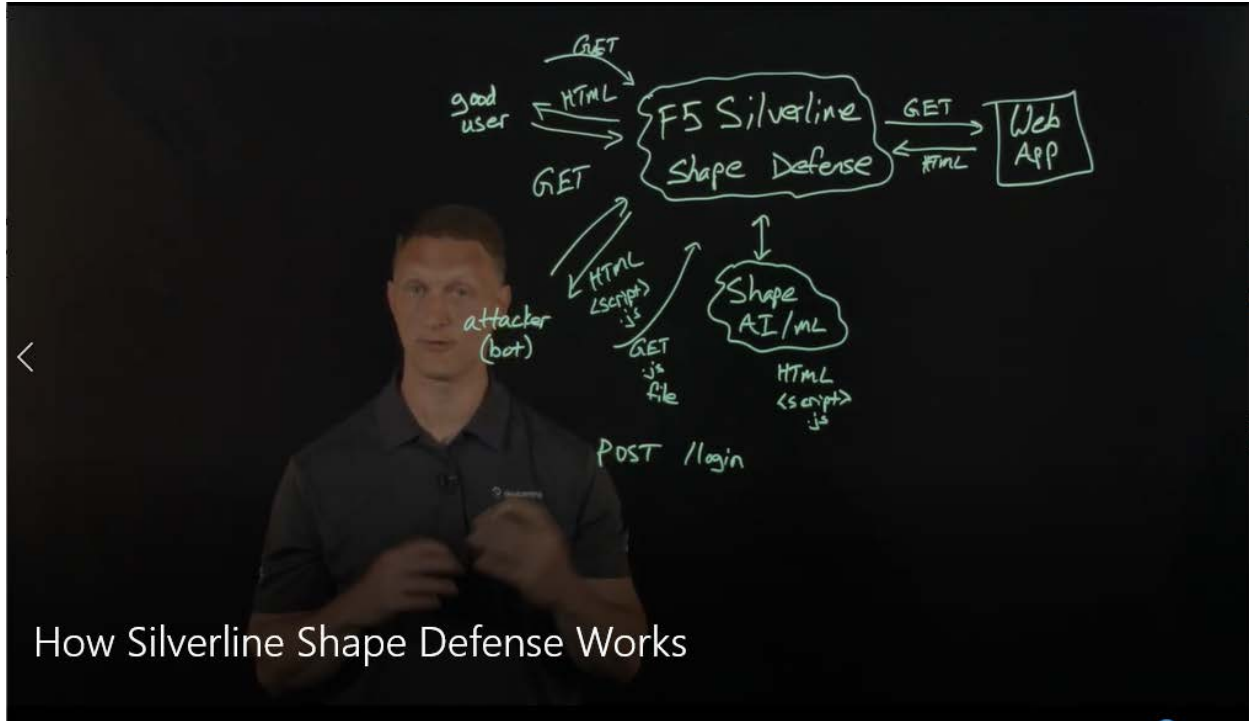
Ex. 26, Shape Enterprise Defense, *available at* <https://www.shapesecurity.com/shape-enterprise-defense> (last visited Jan. 15, 2021).

153. According to F5, Silverline Shape Defense protects online applications from automated bot attacks wielding advanced threats like credential stuffing, unwanted scraping, carding and automation traffic to penetrate company defenses. Ex. 29, Silverline Shape Defense,

available at <https://www.f5.com/products/security/silverline/shape-defense> (last visited Jan. 15, 2021); Ex. 30, F5 Silverline Shape Defense, available at <https://www.f5.com/pdf/products/f5-silverline-shape-defense-datasheet.pdf> (last visited Jan. 15, 2021). According to F5, Silverline Shape Defense leverages Shape technology. Ex. 29, Silverline Shape Defense, available at <https://www.f5.com/products/security/silverline/shape-defense> (last visited Jan. 15, 2021).



Ex. 29, Silverline Shape Defense, available at <https://www.f5.com/products/security/silverline/shape-defense> (last visited Jan. 15, 2021).



How Silverline Shape Defense Works, F5 DevCentral (June 1, 2020), available at <https://www.youtube.com/watch?v=wJS5xDfyAs4>.

154. F5 represented in its Annual Report that:

Silverline provides customers fully-managed application security. Current offerings include Silverline Web Application Firewall, Silverline DDoS Protection, and Silverline Threat Intelligence Services. These services provide enterprise and service provider customers with F5’s proven security technologies coupled with world-class security professionals. Silverline’s Security Operations Center experts set up, manage, and support each customer’s application solutions as an extension to the customer’s staff. Shape technology was combined in F5’s fiscal third quarter with F5’s Silverline managed services platform to launch Silverline Shape Defense, creating a version of Shape’s technology platform capabilities for customers who prefer a managed service.

Ex. 17, Annual Report, Form 10-K, at 6 (Certified Nov. 13, 2020).

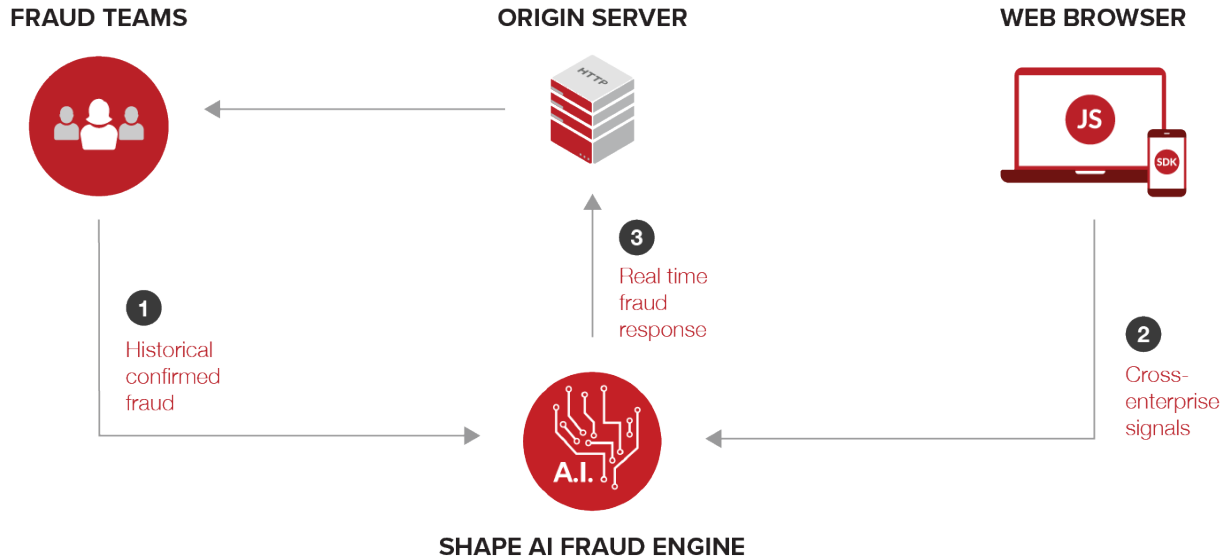
155. F5 further represented in its Annual Report that:

Shape’s technology platform enables generalized AI-powered user analytics. While Shape has focused on using these capabilities to detect advanced fraud and abuse, going forward, the same technology is being integrated throughout F5 to create

general AI-powered user analytics capabilities within and beyond cybersecurity use cases.

Id.

156. According to F5, Shape AI Fraud Engine, which is utilized and integrated into Shape Defense, is focused on understanding intent and connects context across different browsers and devices used by the same user, as well as observations from across Shape's entire network. Ex. 31, Shape AI Fraud Engine, *available at* <https://www.shapesecurity.com/shape-ai-fraud-engine> (last visited Jan. 15, 2021); Ex. 32, SAFE – Shape AI Fraud Engine, *available at* <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20AI%20Fraud%20Engine-Product%20Datasheet.pdf> (last visited Jan. 15, 2021). Shape AI Fraud Engine feeds this data and enterprise fraud files into an AI engine that determines a single, high-fidelity, real-time outcome. *Id.* Shape AI Fraud Engine delivers fraud reductions immediately and continues to drive fraud down more and more in each successive month as the engine consumes more data. *Id.* The application leverages the technology acquired from Shape. Ex. 33, F5 Networks intros new fraud detection engine based on Shape Security acquisition (Oct. 6, 2020), *available at* <https://www.zdnet.com/article/f5-networks-intros-new-fraud-detection-engine-based-on-shape-security-acquisition/> (last visited Jan. 15, 2021).

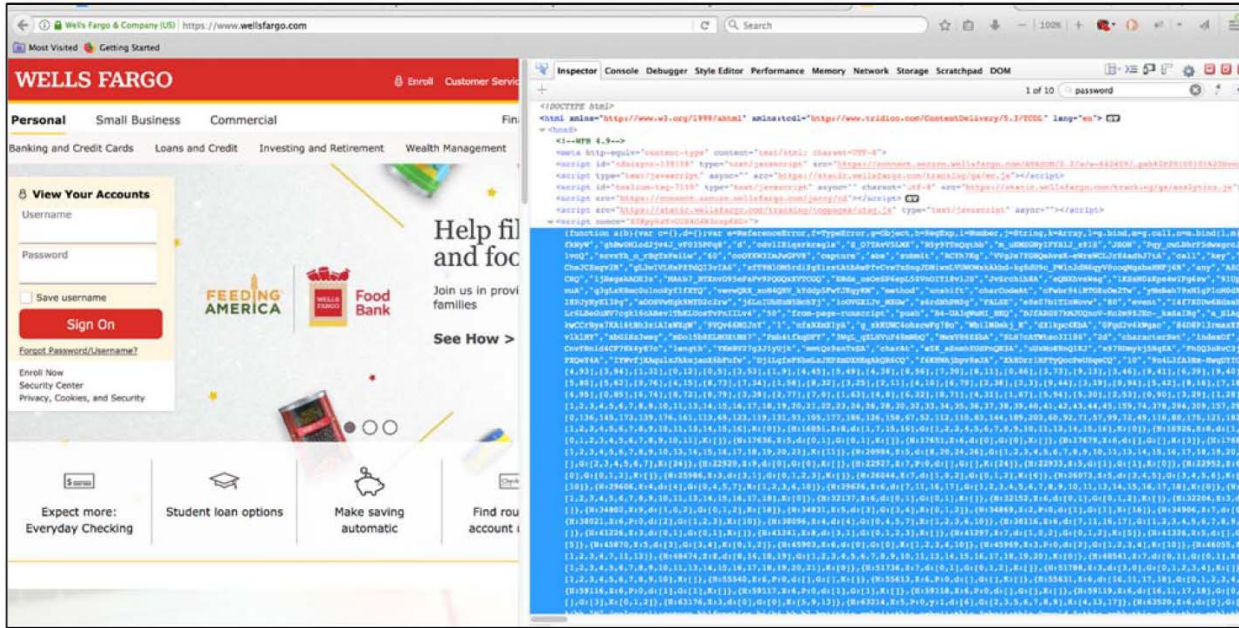


Id.

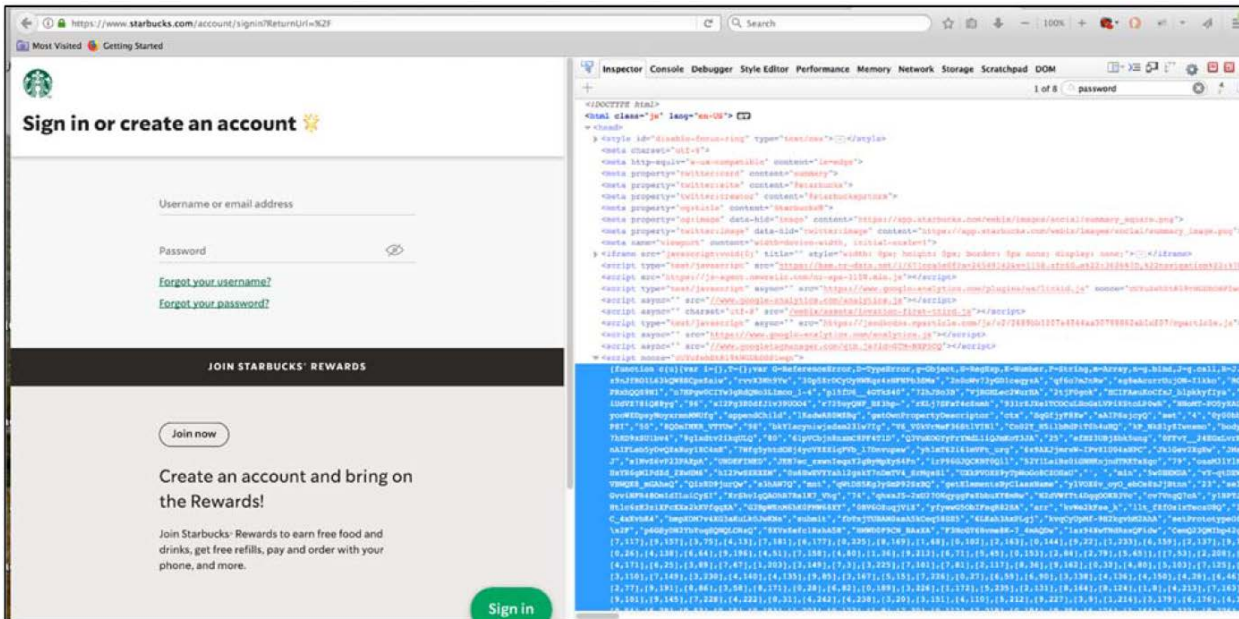
157. F5 products, apps, and websites change their source code constantly, to prevent automated attacks. A review of source code from the corporate websites of F5 customers reveals the use of F5 technology. For example, source code from the corporate websites of Starbucks Corp. and Wells Fargo & Company was collected on December 31, 2019. Similarly, source code was collected on January 6, 2021, from the corporate website of Capital One. *See* Ex. 34, *available at* <https://www.shapesecurity.com/web-application-security/starbucks> (last visited Jan. 21, 2021); Ex. 35, *How Starbucks Combats Account Takeover (ATO)* (June 28, 2018), *available at* <https://blog.shapesecurity.com/2018/06/28/how-starbucks-combats-account-takeover-ato/>; Ex. 36, *Shape Security Raises \$26M As Cybersecurity Puts More Money In The Bank* (Nov. 1, 2018), *available at* <https://news.crunchbase.com/news/shape-security-raises-26m-as-cybersecurity-puts-more-money-in-the-bank/> (last visited Jan. 15, 2021); Ex. 6, *Open Banking*, *available at* <https://www.f5.com/solutions/banking-and-financial-services/open-banking> (last visited Jan. 15, 2021).

158. One feature of the F5 Shape Defense and Shape Enterprise Defense products is the protection of applications and websites by changing their source code constantly, to prevent

automated attacks. A review of source website code for the corporate websites of Starbucks Corp. and Wells Fargo & Company reveals the use of this functionality.



Ex. 37, Correspondence from D. Majewski to Shape Security at 5 (Jan. 14, 2020).



Id. at 6.

See Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 14, 2021).

160. Shape filed patent applications directed to the above-referenced technology beginning in March 2013, with later, more substantive filings directed to the same subject matter filed in 2014 and 2015.

F5'S INFRINGEMENT OF SUNSTONE'S PATENTS

161. F5 has infringed and continues to infringe one or more claims of each of the '870 and '759 Patents and the '537 Application (the "Asserted Patents") by engaging in acts that constitute infringement under 35 U.S.C. § 271, including but not necessarily limited to making, using, selling, and/or offering for sale, in this district and elsewhere in the United States, and/or importing into this district and elsewhere in the United States, the Shape Connect, ShapeShifter Elements, Shape Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and Silverline Shape Defense, alone or in conjunction with one another (collectively, "the Accused Products").

162. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, F5 indirectly infringes all the Asserted Patents by instructing, directing and/or requiring others, including its customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Asserted Patents.

163. F5 has willfully infringed the '870 and '759 Patents. SunStone is informed and believes that F5, either alone or through Shape, had knowledge of the Asserted Patents through various channels and despite its knowledge of SunStone's patent rights, engaged in egregious behavior warranting enhanced damages.

164. Shape submitted a provisional patent application, United States Provisional Patent Application Serial No. 61/801,142 (the “Shape ’142 Application”), directed to subject matter substantially similar to that claimed in the Asserted Patents and also to that developed and marketed by SunStone on March 15, 2013. In the Shape ’142 Application, the inventors used the term “random,” rather than “polymorphism” to describe their invention, where 32 of those references were to “random” changes to the page. Similarly, Shape filed additional patent applications in October 2013, which used the term “random ways” to describe their purported invention.

165. At the time of the filing of the Shape ’142 Application., Shape did not use the term “polymorph” or any derivative in its patent applications, which is consistent with its description in the press:

Our technology uses a unique approach to security which has demonstrated extremely high efficacy against some of the most serious attacks today, such as Man-in-the-Browser,” said co-founder Sumit Agarwal in an email to VentureBeat. “The demand from customers has been so high that we have raised a Series B to invest more and move even faster.”

Ex. 38, Shape Security gets \$20M second round while still not revealing its products (Jan. 7, 2013), *available at* <https://venturebeat.com/2013/01/07/shape-security-funding/> (last visited Jan. 15, 2021).

166. The above-referenced article further stated:

Shape also has well-respected security investors on its board, including KPCB’s Ted Schlein, known for being an early employee in antivirus giant Symantec, among other accomplishments.

Id.

167. Ted Schlein is a General Partner at Kleiner Perkins Caufield & Byers. *See* Ex. 39, Ted Schlein Bio, *available at* <https://www.kleinerperkins.com/people/ted-schlein/> (last visited Jan.

15, 2021). Mr. Schlein was an investor in in Shape and was a member of its Board of Directors. See Ex. 40, Forbes Profile, available at <https://www.forbes.com/profile/ted-schlein/?sh=298dd0af3532> (last visited Jan. 15, 2021); Ex. 41, LinkedIn Profile (last visited Jan. 14, 2021).

168. In November 2013, Dr. Ford reached out to Ted Schlein at Kleiner Perkins in an effort to gauge interest in potential investment in SunStone. Attached to the email was a “one-pager,” describing SunStone’s solution:

SunStone is a server-side approach to e-Commerce session integrity that detects virus activity at client endpoints. It does this by hijacking the hard, computer science problems of “virus polymorphism” and “zero-day” vulnerability and puts them to work for the defense!

...

The components are not static but “polymorphic”: they may be redesigned and repackaged in a great variety of ways and still maintain their original functionality. This effectively turns the tables and presents the virus polymorphism problem as a challenge for the bad guys.

Ex. 42, Email from D. Ford to T. Schlein and attachments (Nov. 26, 2013).

169. Beginning in December 2013, Shape’s patent applications began referencing “polymorphism” and began to deemphasize the usage of “random.” Similarly, the press descriptions of Shape began to highlight the use of polymorphism, similar to the “one-pager” that Dr. Ford sent to Schlein:

Botnets can’t be stopped largely because the bad guys have mastered a technique, called polymorphism, by which they continually tweak the underlying malicious code to stay a step ahead of the latest security updates.

Shape's co-founders came up with the notion of using polymorphism against the bad guys. Shape's technology doesn't bother trying to detect botnet activity. Instead, it continually scrambles the exchange of information taking place between a Web server and a Web site visitor, be it a legit user or a malicious bot.

Gartner banking security analyst Avivah Litan credits Shape for breaking new ground. “You’ve got to hand it to them, they did something revolutionary, and you don’t see revolutionary technology very often,” Litan says. “No one ever comes up

with new ideas in security. It's always variations of old ideas and incremental changes.”

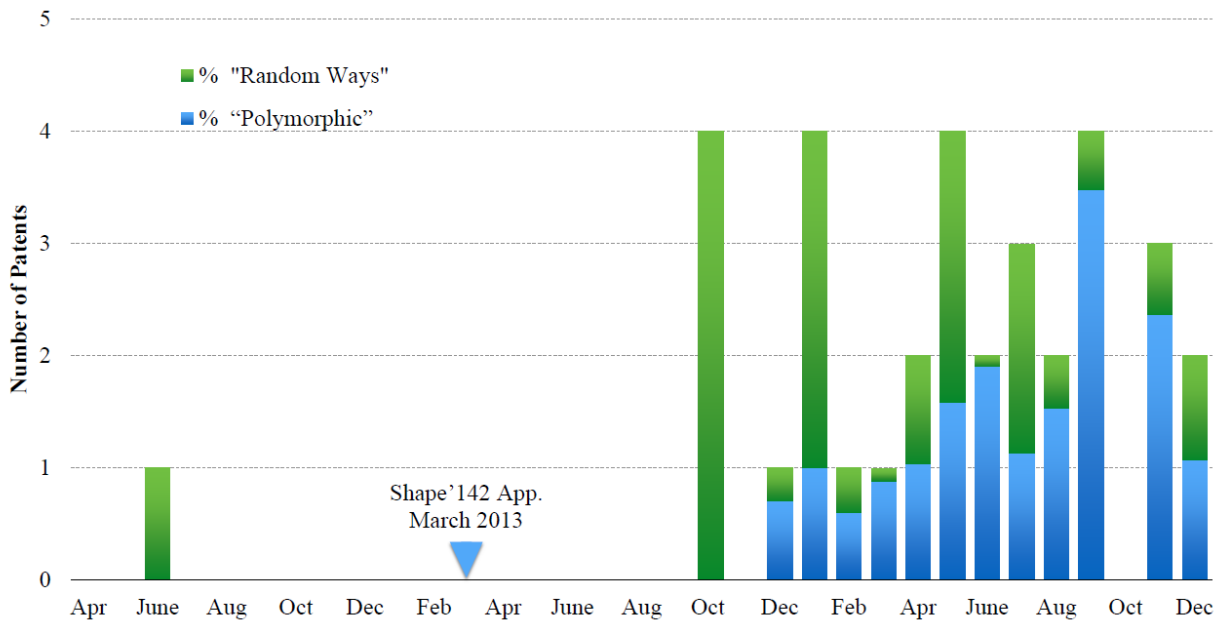
...

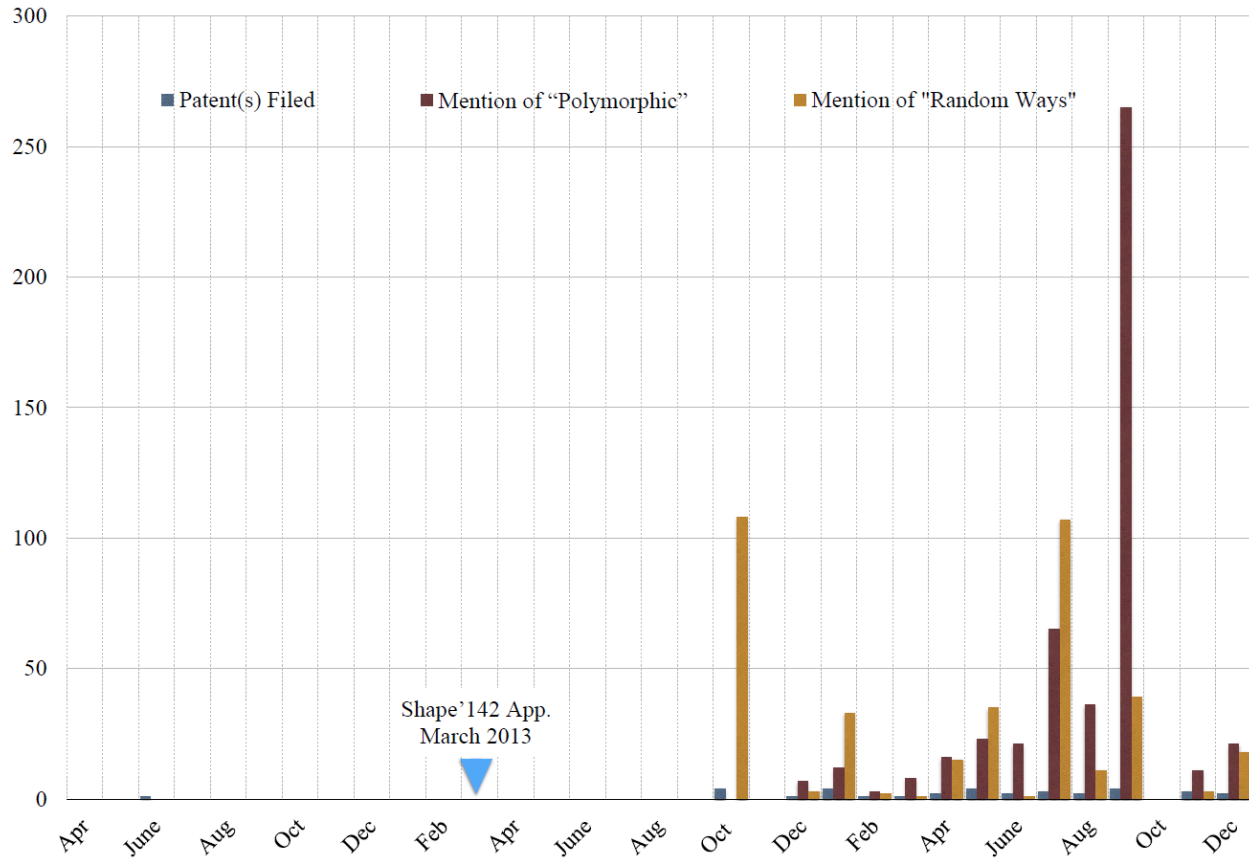
Ted Schlein, a managing partner at Kleiner Perkins Caufield & Byers, says Shape has concocted the Internet's first “botwall.”

“What the world needs is a new tier of security architecture that blocks all commands from bots, malware and scripts,” Schlein says. “Shape has successfully created the world's first botwall. The Internet badly needs this.”

Ex. 43, Can Shape Security revolutionize Web defense? (Jan. 21, 2014), available at <https://www.usatoday.com/story/cybertruth/2014/01/21/can-shape-security-revolutionize-web-defense/4656467/> (last visited Jan. 21, 2021).

170. This change in direction by Shape, from “random” to “polymorph,” is further shown in the graph below detailing the use of the terms in Shape patents:





171. On January 21, 2014, Shape launched its ShapeShifter product. Ex. 44, Introducing the Shape Shifter (Jan. 21, 2014), *available at* <https://blog.shapesecurity.com/2014/01/21/introducing-the-shape-shifter/> (last visited Jan. 15, 2021).

172. Shape described the product as:

The ShapeShifter uses real-time *polymorphism* as a defense—it dynamically changes website code to break automated attacks. Cybercriminals have long used *polymorphism* to hide malware by making the malware appear to be different upon every new infection. We harness *polymorphism* to make the source code of websites appear differently on every page view, which has the effect of defeating malware, botnets and scripts. All of this happens without creating any user-visible changes. The website looks and feels exactly the same to legitimate users, but the underlying site code (HTML, JavaScript, and CSS) is different on every pageview. Because bots must reference the content in some manner, this never-ending modulation of the site code breaks scripts and deflects attacks. Ultimately, the ShapeShifter aims to stop non-human visitors from executing large-scale

automated attacks. This may help break the economics of breaches like the one Target experienced in late 2013, by eliminating the monetization path.

Id. (emphasis added).

173. On January 14, 2020, SunStone’s counsel sent Shape notice that Shape was “infringing some of Sunstone’s critical intellectual property, and in particular Shape Security is infringing some of Sunstone’s patents related to network and device security.” *See* Ex. 37, Correspondence from D. Majewski to Shape Security at 1 (Jan. 14, 2020) (the “Notice Letter”).

174. The Notice stated:

Based on Sunstone’s diligent investigation to date, it appears that Shape Security has a nearly identical security product that is disclosed in the above-referenced patents and that Shape Security’s product infringes Sunstone’s patents. In the past, Shape Security has referred to this feature as “Shapeshifter”, “polymorphism”, and “transmutation”. The claim chart below shows one example of Shape Security’s infringement—in particular, the claim chart shows how Shape Security infringes Claim 15 of U.S. Patent No. 10,230,759 using the latest available information from Shape Security’s 2016 website.

Id.

175. The Notice Letter further included claim charts detailing the infringement of at least ShapeShifter Elements. *Id.* at 2-4. The Notice Letter concluded that “Shape Security is presently infringing at least Sunstone’s website security patents referenced above,” which includes the ’870 and ’759 Patents. *Id.* at 5.

176. The Notice Letter included additional details of Shape’s infringement, including screen shots of website source code for Starbucks Corp. and Wells Fargo & Company. *Id.*

177. The Notice Letter further noted that SunStone first filed the above-described feature with the U.S. Patent and Trademark Office on September 21, 2011. Shape Security did not file a patent application directed to the same subject matter until March 15, 2013, with later more substantive filings directed to the same subject matter being filed in 2014 and 2015.” *Id.* at 6.

178. F5 completed the acquisition of Shape on January 24, 2020. SunStone is informed and believes that F5 gained knowledge of at least the '870 and '759 Patents as a result of the acquisition of Shape.

179. SunStone is informed and believes that despite F5 and Shape's knowledge of the Asserted Patents and SunStone's patented technology, F5 and Shape made the deliberate decision(s) to sell products and services that each knew infringe SunStone's Asserted Patents.

180. SunStone is informed and believes that F5 has undertaken no efforts to avoid infringement of the Asserted Patents, despite F5's knowledge and understanding that F5's products and services infringe these patents. Thus, F5's infringement of Asserted Patents is willful and egregious, warranting enhancement of damages.

181. SunStone is informed and believes that F5 knew or was willfully blind to the Asserted Patents and their infringement thereof. Despite this knowledge and/or willful blindness, F5 has acted with blatant and egregious disregard for SunStone's patent rights with an objectively high likelihood of infringement.

182. Shape's infringing actions have negatively affected SunStone's business. For example, SunStone was in contact with Wells Fargo & Company in mid-January 2015. Shortly after its contact with SunStone, Wells Fargo & Company implemented a very similar solution to SunStone's proposed solution using Shape's products. Similarly, Shape lost business with the National Security Agency (SunStone first proposed a solution in March 2015), Nike, Inc. (SunStone first proposed a solution in September 2015), and the potential acquirer Imperva (SunStone first proposed a solution in March 2016). Shape's infringement has been a significant factor in undercutting SunStone's technology advantage and, thus, the ability to acquire customers.

183. Also, before F5 or Shape was aware of the technology, SunStone filed its patent applications regarding the conversion, injection, or transformation of webpage code into a format that prevents interference by a malicious system. More specifically, SunStone filed a provisional application covering the above-described feature with the United States Patent and Trademark Office on September 21, 2011. Shape did not submit a patent application directed to the same subject matter until March 15, 2013, with subsequent filings filed in 2014 and 2015.

CAPITAL ONE

184. Capital One was founded in 1994 in Richmond, Virginia.

185. Capital One is an American bank holding company specializing in credit cards, auto loans, banking, and savings accounts, headquartered in McLean, Virginia with operations primarily in the United States. *See* Ex. 45, Capital One IR Overview, *available at* <https://ir-capitalone.gcs-web.com/investor-relations?c=70667&p=irol-irhome> (last visited Jan. 15, 2021).

186. Capital One is the twelfth largest bank in the United States and has developed a reputation for being a technology-focused bank. *See* Ex. 46, FDIC Quarterly, *available at* <https://www.fdic.gov/bank/analytical/quarterly/index.html> (last visited Jan. 15, 2021).

187. With a market share of 5%, Capital One is also the second largest auto finance company in the United States. *See* Ex. 47, Ally Financial leads in Q2 auto loan market share, Experian says (Oct. 10, 2018), *available at* https://www.autonews.com/article/20181010/FINANCE_AND_INSURANCE/181019869/ally-financial-leads-in-q2-auto-loan-market-share-experian-says (last visited Jan. 15, 2021).

THE ACCUSED CAPITAL ONE PRODUCTS AND SERVICES

188. The Shape Enterprise Defense product is used by eight of the top 12 US banks, including Capital One. *See* Ex. 27, New Product Protects SMBs From Credential Stuffing Attacks

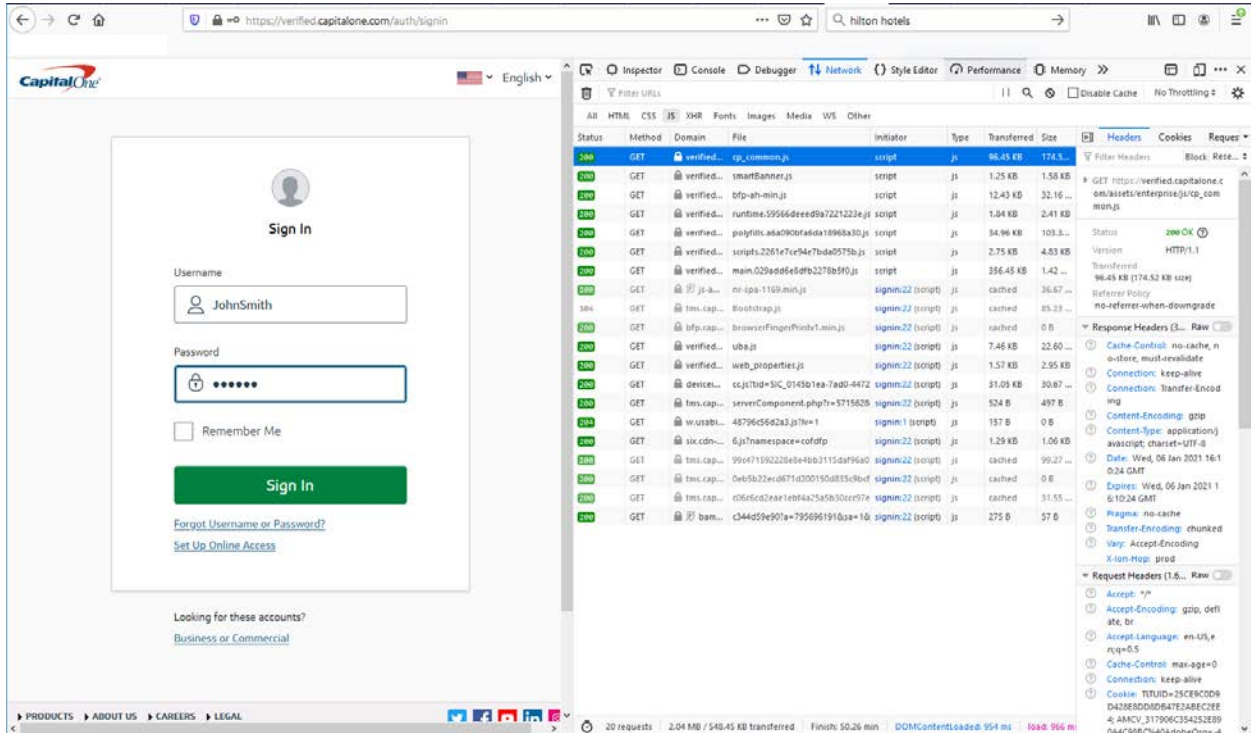
(May 8, 2019), *available at* <https://www.securityweek.com/new-product-protects-smbs-credential-stuffing-attacks> (last visited Jan. 15, 2021). As noted above, Shape Enterprise Defense uses the Shape Defense Engine in conjunction with the Shape AI Cloud. Ex. 26, Shape Enterprise Defense (last visited Jan. 7, 2020), *available at* <https://www.shapesecurity.com/shape-enterprise-defense> (last visited Jan. 15, 2021).

189. Capital One is a customer of F5 and will have information relevant to SunStone's claims of infringement. According to F5:

In many open banking applications, every millisecond matters. With F5, you can achieve previously impossible speeds through real-time APIs. Take Capital One's developer portal. F5 technology has enabled them to scale applications to 12 billion operations per day, with peaks of 2 million operations per second at latencies of just 10–30 milliseconds.

Ex. 6, Open Banking, *available at* <https://www.f5.com/solutions/banking-and-financial-services/open-banking> (last visited Jan. 15, 2021).

190. A review of source website code for the corporate website of Capital One demonstrate that the website obfuscates the source code constantly, to prevent automated attacks.



Capital One Customer Sign In Webpage, available at <https://verified.capitalone.com/auth/signin> (last visited Jan. 14, 2021).

191. Capital One’s use of Shape Enterprise Defense is shown in the first line of the code of the Java Script file `cp_common.js`:



Id.

CAPITAL ONE’S INFRINGEMENT OF SUNSTONE’S PATENTS

194. Capital One has infringed and continues to infringe one or more claims of each of the Asserted Patents by engaging in acts that constitute infringement under 35 U.S.C. § 271, including but not necessarily limited to using in this district and elsewhere in the United States methods, systems, and apparatuses that infringe the Asserted Patents.

195. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Capital One indirectly infringes all the Asserted Patents by instructing, directing and/or requiring others, including its customers and users, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Asserted Patents.

196. Capital One has willfully infringed each of the Asserted Patents. SunStone is informed and believes that Capital One had knowledge of the Asserted Patents through various

channels and despite its knowledge of SunStone's patent rights, engaged in egregious behavior warranting enhanced damages.

197. One or around May 2015, Jeff Newman, Chairman of SunStone's Board of Directors at the time, reached out to Tony Spinelli at Capital One on behalf of SunStone.

198. Mr. Newman notified Mr. Spinelli, in part, that:

SunStone aggressively targets Advanced Persistent Threats (polymorphic, trojan viruses, APTs). Three years stealth in the making (*IP and patents*), SunStone is unique "inside-the-session Active Defense" and proactively tackles pain of persistent viral attack, embed programs (APT, polymorphisms). Aggressive inner session defense through constantly changing polymorphic booby-traps with live analysis. Biodiverse advantages, delivered as IP and a service. Easily scales to any industry segment, enterprise to mid-market, commercial to fed gov or SLED.

Ex. 48, Email Chain Between SunStone and Capital One (May 26, 2015, through August 23, 2015) (emphasis added).

199. Over the course of the next three months, SunStone spoke with or presented via demonstration the SunStone technology to numerous individuals at Capital One, including Tony Spinelli, Nami Mufti, Erik Rolf, Denice Roach, Adam Boutin, and Ivan Ferko. *Id.*

200. SunStone was informed on August 23, 2015, that Capital One did "not wish to further engage in discussions with SunStone." *Id.*

201. SunStone is informed and believes that despite Capital One's knowledge of the Asserted Patents and SunStone's patented technology, Capital One made the deliberate decision(s) to sell products and services that it knew infringe SunStone's Asserted Patents.

202. SunStone is informed and believes that Capital One knew or was willfully blind to SunStone's technology and the Asserted Patents. Despite this knowledge and/or willful blindness, Capital One has acted with blatant and egregious disregard for SunStone's patent rights with an objectively high likelihood of infringement.

203. SunStone is informed and believes that Capital One has undertaken no efforts to avoid infringement of the Asserted Patents, despite Capital One's knowledge and understanding that Capital One's products and services infringe these patents. Thus, Capital One's infringement of the Asserted Patents is willful and egregious, warranting enhancement of damages.

FIRST CAUSE OF ACTION

(F5's Direct Infringement of the '870 Patent pursuant to 35 U.S.C. § 271(a))

204. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

205. F5 has infringed and continues to infringe at least Claims 1-20 and 37-38 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 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).

206. F5's infringing Accused Products include, without limitation, Shape Connect, ShapeShifter Elements, Shape Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and Silverline Shape Defense and other solutions with the same or similar features and functionality that satisfy each element of one or more asserted claims. Each of the above-referenced Accused Products incorporates or builds upon Shape Defense.

207. F5'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.

208. The Accused Products embody the patented invention of the '870 Patent and infringe the '870 Patent because they practice a method comprising:

receiving, in a security server from a transaction server, transactional information to transmit to a client device based on a transaction with the client device;

receiving, in the security server from the transaction server, presentation information corresponding to the transactional information;

modifying, via the security server, at least some of the presentation information;

transmitting, via the security server, the modified presentation information and transactional information to the client device;

determining, via the security server, an acceptable response based on i) the modified presentation information and the transactional information, ii) how the client device is configured to render the transactional information, and iii) predicted response information associated with the transactional information that is expected to be provided by a user of the client device; and

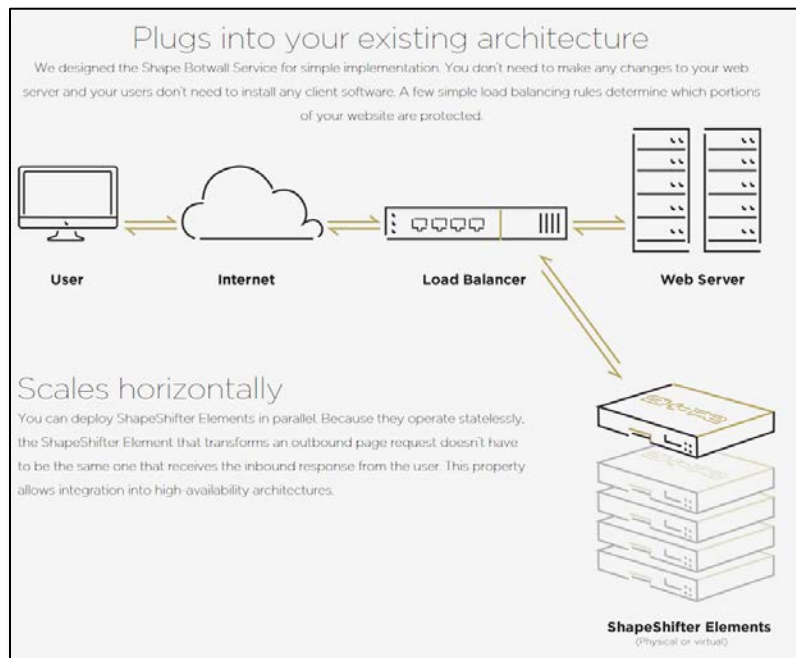
responsive to information in a response message from the client device not matching the acceptable response, providing an indication there is a malicious application affecting communications between the transaction server and the client device, wherein the acceptable response is further determined based 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 39.

209. According to F5 and historical Shape documentation, the Accused Products utilize the Shape Defense platform. As shown by historical Shape documentation, the Accused Products perform a method using a security server. For example, ShapeShifter Elements performs a method using a security server, functioning as a Shape Botwall Service, located between the web server and the client user. Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at*

<https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021). Prior to being launched as ShapeShifter Elements, the Shape product was known as PolyRef and was presented in a technical paper as early as June 2014. Ex. 50, Xinran Wang, et al., Polymorphism as a Defense for Automated Attack of Websites at 513–530 (Springer International Publishing, Switzerland 2014).

210. The Accused Products receive in a security server from a transaction server, transactional information to transmit to a client device based on a transaction with the client device. For example, the transactional server sends the transactional information to the security server. Transactional information includes at least the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login. In this configuration, ShapeShifter Elements can be a virtual server (determined in discovery) being functionally provided through software implementation rather than a physical device (i.e., SAAS).



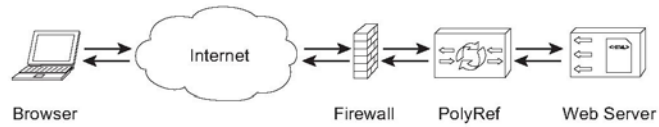


Fig. 1. PolyRef as a transparent proxy

Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021); Ex. 50, Xinran Wang, et al., *Polymorphism as a Defense for Automated Attack of Websites* at 513–530 (Springer International Publishing, Switzerland 2014).

211. F5 now refers to ShapeShifter Elements as Shape Defense, which includes the functionality of ShapeShifter Elements. Shape Defense offers greater coverage and tracking but still focuses on preventing sophisticated bot attacks on key web pages. The key web pages protected include login and checkout but cover other key pages so that Shape Defense can prevent bots from Account Takeover, Carding, Inventory Hoarding, Scraping, Gift Card Attacks and Marketing Fraud.



ATTACKS ON WEBSITES AND MOBILE APPS DRIVE FRAUD, RISK, AND BAD CUSTOMER EXPERIENCES

Every day, web and mobile applications face an onslaught of sophisticated attacks with one commonality: instead of exploiting application vulnerabilities, attackers abuse an application's functionality as it was intended for legitimate users. These imitation attacks - delivered by bots and other forms of automation - simulate human behavior using highly sophisticated attack tools, with the goal of conducting crime or disrupting business.

Shape Defense protects online businesses from such sophisticated attacks that would otherwise result in large scale fraud. Companies get the visibility, detection and mitigation outcomes they need to slash fraud, reduce cloud hosting, bandwidth and compute costs, improve user experiences, and optimize their business based on real human traffic.



WORLD-CLASS PROTECTION

Designed to meet the needs of a broad range of organizations, Shape Defense delivers world-class application protection that leverages the power of the Shape network.

AI-powered: Through the use of advanced AI and ML, Shape Defense accurately determines in real-time if an application request is from a fraudulent source and when it is, mitigates, while allowing legitimate human users without introducing additional friction.

Collective defense: Shape Defense customers benefit from everything Shape learns through the large protection network we operate. Every 24 hours, Shape blocks more than one billion fraudulent log-in attempts and other transactions, while ensuring that more than 150 million legitimate human transactions are kept safe.

Omnichannel protection: Shape Defense can be deployed to protect web and mobile applications, as well as HTTP APIs. The company's mobile SDK is deployed on more than 200 million iOS and Android devices worldwide.

Easy to deploy and flexible to implement: Shape Defense can be implemented in a variety of modes, including deployments as quick as 30 minutes, to suit the needs of the organization and to best mitigate any attack traffic the business experiences. And Shape Defense is managed through simplified administration that does not tax your security team to operate.

PROTECTION AGAINST BOTS AND OTHER AUTOMATION ATTACKS

Shape Defense protects against the most sophisticated credential stuffing, account take over attacks, carding, and the rest of the OWASP Automated Threats to Web Applications list. Shape Defense delivers continuous protection even when attackers retool, ensuring durable protection is sustained.

Account Takeover

Stop fraudsters from rapidly testing stolen credentials on your login applications, which means they can't take over accounts in the first place.

Inventory Hoarding

Ensure your campaigns and most in-demand items are sold directly to your customers, not to scalpers.

Gift Card Attacks

Ensure gift card value, loyalty points and other stored value remains in your customers' hands.

Carding

Prevent criminals from using your checkout pages to validate stolen credit cards.

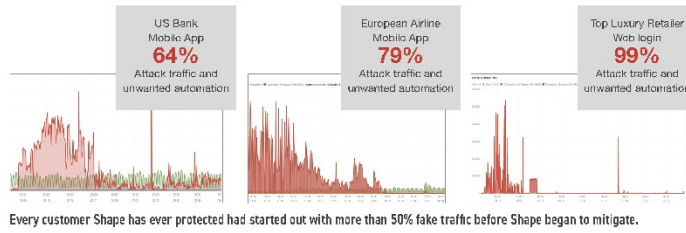
Scraping

Control how scrapers and aggregators harvest data from your website, allowing you to protect sensitive data and manage infrastructure costs.

Marketing Fraud

Ensure your business analytics and marketing spend are driven by real human users and not automated bots.

shapesecurity.com sales@shapesecurity.com +1 (505) 389-0400

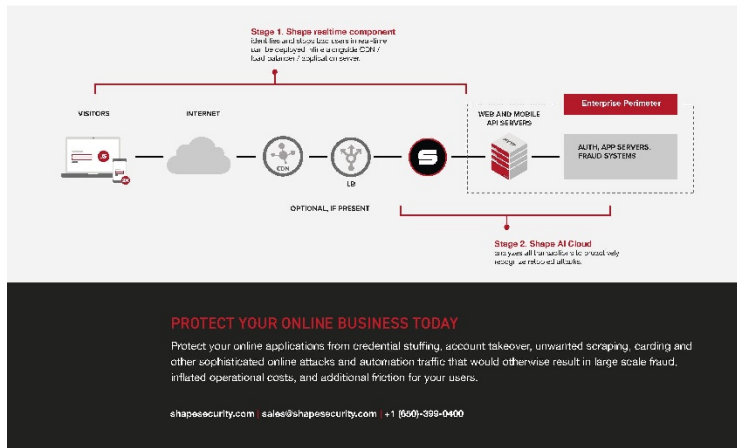


HOW SHAPE DEFENSE WORKS

Shape Defense uses a patented two-stage process to deliver highly accurate real-time detection and mitigation, as well as to provide sustained protection through attacker rotation.

Stage 1 evaluates each transaction across a set of proprietary risk factors that include network, activity, user, device and account factors. These risk factors are evaluated in light of everything Shape has learned across its global customer base. Shape's innovative Stage 1 sees all traffic - including mitigated automation traffic - and also includes insights learned from detecting fraudulent activity across other Shape clients (aggregated defense from aggregated insights).

Shape's unique Stage 2 defense counters the attackers' evolution with an after-action machine learning and human analysis. Specifically, our Stage 2 defensive system leverages three tiers of supervised and unsupervised learning and provides unparalleled protection. Shape AI Cloud analyzes all transactions to proactively recognize rotation attacks.



Ex. 23, 2020 Shape Defense Datasheet, available at <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

212. According to F5 and historical Shape documentation, the Accused Products receive, in the security server from the transaction server, presentation information corresponding to the transactional information. For example, the security server also receives presentation information used to display and interact with the transactional information on the web page. The presentation information is soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. See Ex. 49, The Shape Botwall Service (Sept. 10, 2015), available at

<https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

213. According to F5 and historical Shape documentation, the Accused Products modify, via the security server, at least some of the presentation information. For example, as shown in the F5 and historical Shape documentation, the soft information coding is the information that a bot might search and then discover, i.e., the type of information that is being requested so that the bot can respond with stolen usernames and passwords. The presentation information is described, in part, by specifying the explicit form “login_form.php” and the explicit variables needed for the form - “username” and “password.” A combination of presentation and transaction information that is an indication of the data fields and data/text requested to be displayed to acquire a password and a user ID / username (transaction or hard information).

An example countermeasure:
reference polymorphism

How do you change the very nature of HTML, to introduce a new security model, while still delivering open markup code to web browsers? Shape transforms pages in real-time to introduce polymorphic code which presents barriers which are difficult or impossible for attackers to overcome. Here's one simple example of code before and after being protected by the Shape Botwall Service:

ORIGINAL WEBSITE CODE (BEFORE)	TRANSFORMED WEBSITE CODE (AFTER)
<pre><form action="login_form.php"> <input id="username" name="username"/> <input id="password" name="password"/> <input type="submit"/> </form></pre> <p style="text-align: right; font-size: small;">Simplified HTML</p>	<pre><form action="R6bYEc2taB4e"> <input id="bNoeTn2bjf2F" name="p5Tb6SGCf63g"/> <input id="k5KbSjCT6p4t" name="yWTg3L082t2f"/> <input type="submit"/> </form></pre>

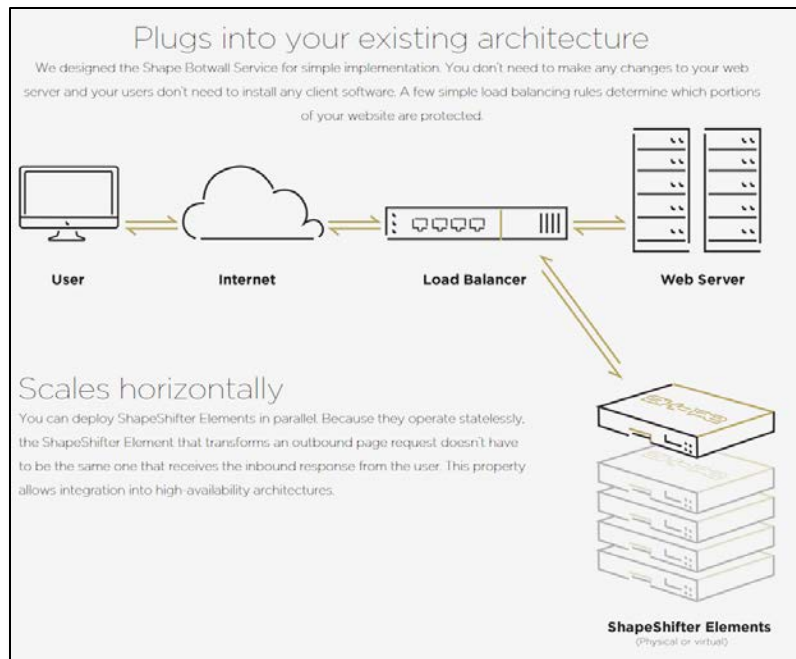
Id.

214. In the Accused Products, the first set of website code is transformed to obscure the web server's name for the form (presentation information) used and the form's transactional information entries requested. For example, the original form requested was “login_form.php” and is now replaced by the text string “R6bYEc2taB4e”. A transformation table is kept in the

security processor to inverse transform back to the necessary labels for the web server. In this example, the Accused Products, obscure “login_form” and “username” and “password” and transformed the fields into “bNoeTn2bjf2F” and “p5TbGSGCf63g” for “username” and “k5KbSjCT6p4t” and “yWTg3LO82t2f” for “password.”

215. According to F5 and historical Shape documentation, the Accused Products transmit, via the security server, the modified presentation information and transactional information to the client device. For example, after the Security Server has obscured the presentation information, the modified HTML code for the web page is sent through the internet and on to the client device for rendering on the client’s display. *Id.*

216. According to F5 and historical Shape documentation, the Accused Products determine, via the security server, an acceptable response based on i) the modified presentation information and the transactional information, ii) how the client device is configured to render the transactional 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, the security server modifies the presentation information to obscure the existence of the transactional information from malicious code. Therefore, an acceptable response must be via the security server to recover the inverse transform. In addition, the type of client display is communicated to the web server as part of the request to visit the web page. The HTML presentation information code must be anchored to the display device and pixel locations become important. Finally, the transactional information such as user ID / username and password must match the registered security information for the client.

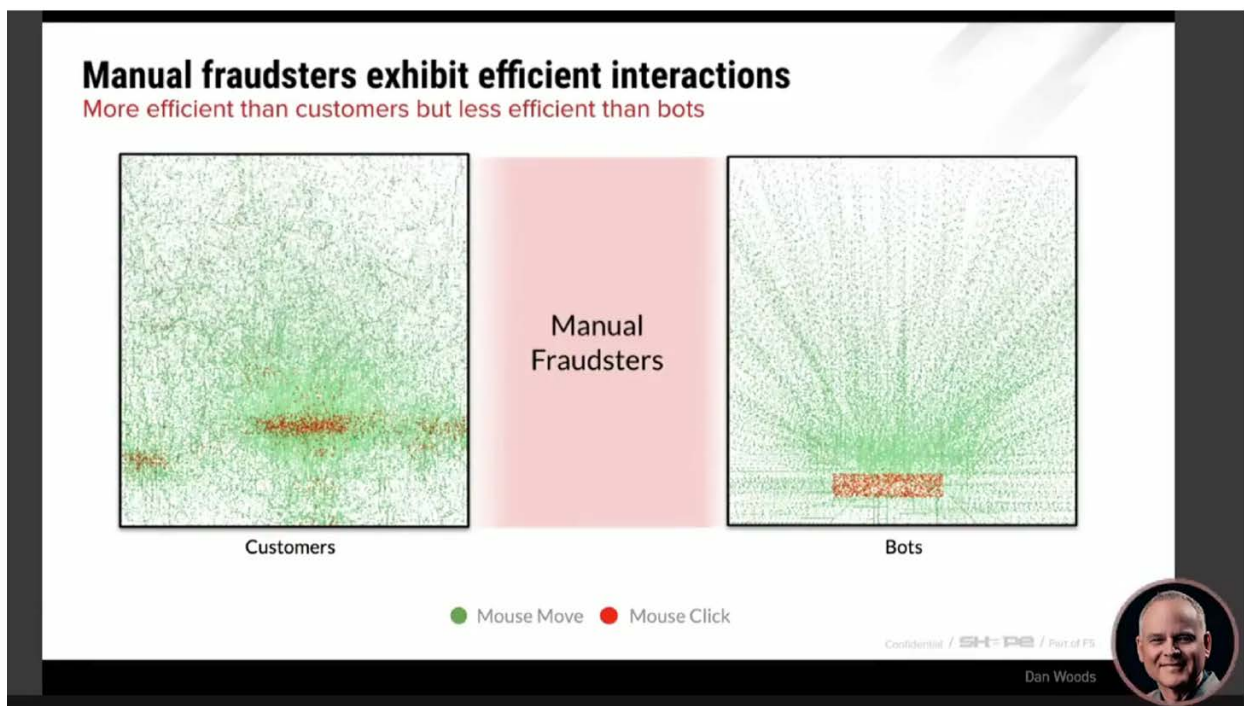


Id.

217. According to F5 and historical Shape documentation, the Accused Products receive the response message from the client device and responsive to information in a response message from the client device not matching the acceptable response, provide an indication there is a malicious application affecting communications between the transaction server and the client device. In the Accused Products a response message is detected and blocked from returning to the web server due to the detection of an unacceptable response when a response message contains code that does not logically follow (i.e., acceptable response) from the modified presentation information sent to the client. This type of response is considered an unacceptable response and indicates the presence of a malicious application (bot). For example, “bNoeTn2bjf2F” is the expected response for username. If a bot sent “username” instead of “bNoeTn2bjf2F”, the inverse transform via the security server would not know how to transform “username” since it is not listed in the inverse transform as a starting point. This inability to transform it back to web server

recognizable code is an indication of malicious code (bot) being present and can be detected. *Id.*; see Ex. 23, 2020 Shape Defense Datasheet, available at <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

218. According to F5 and historical Shape documentation, in the Accused Products the acceptable response is further determined by estimating locations of rendered features and functions as displayed by the client device, estimating locations of rendered page geometry of the features and functions, and estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device, as shown below:



Beyond Automated Attacks: Manual Fraud, Genesis & Magecart (Apr. 16, 2020), available at <https://www.brighttalk.com/webcast/12935/393742> (last visited Jan. 15, 2021).

219. According to F5 and historical Shape documentation, in the Accused Products the acceptable response is further determined by estimating a label of the presentation information,

estimating a utilization of a codeword set based on the presentation information and transactional information, or estimating a utilization of a codeword set based on actions taken by at least one of the user and the client device. For example, in the Accused Products, the first set of website code is transformed to obscure the web server's name for the form (presentation information) used and the form's transactional information entries requested. For example, the original form requested was "login_form.php" and is now replaced by the text string "R6bYEc2taB4e". A transformation table is kept in the security processor to inverse transform back to the necessary labels for the web server.

An example countermeasure: reference polymorphism

How do you change the very nature of HTML, to introduce a new security model, while still delivering open markup code to web browsers? Shape transforms pages in real-time to introduce polymorphic code which presents barriers which are difficult or impossible for attackers to overcome. Here's one simple example of code before and after being protected by the Shape Botwall Service:

ORIGINAL WEBSITE CODE (BEFORE)	TRANSFORMED WEBSITE CODE (AFTER)
<pre style="font-family: monospace; font-size: 0.9em;"><form action="login_form.php"> <input id="username" name="username" /> <input id="password" name="password" /> <input type="submit" /> </form></pre> <p style="text-align: right; font-size: 0.8em; color: #888;">Simplified HTML</p>	<pre style="font-family: monospace; font-size: 0.9em;"><form action="R6bYEc2taB4e"> <input id="bNoeTn2bjf2F" name="p5TbGSGCf63g" /> <input id="k5KbSjCT6p4t" name="yWTg3L082t2f" /> <input type="submit" /> </form></pre>

See Ex. 49, The Shape Botwall Service (Sept. 10, 2015), available at <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

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

221. As a result of F5'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.

222. F5's infringement of the '870 Patent has injured and continues to injure SunStone in an amount to be proven at trial.

223. As set forth in paragraphs 163-183, F5 has willfully infringed the '870 Patent. SunStone is informed and believes that F5, either alone or through Shape, had knowledge of the '870 Patent through various channels and despite its knowledge of SunStone's patent rights, engaged in egregious behavior warranting enhanced damages.

224. SunStone is informed and believes that despite F5 and Shape's knowledge of the '870 Patent and SunStone's patented technology, F5 and Shape made the deliberate decision(s) to sell products and services that each knew infringe SunStone's '870 Patent.

225. SunStone is informed and believes that F5 knew or was willfully blind to SunStone's technology and the '870 Patent. Despite this knowledge and/or willful blindness, F5 has acted with blatant and egregious disregard for SunStone's patent rights with an objectively high likelihood of infringement.

226. SunStone is informed and believes that F5 has undertaken no efforts to avoid infringement of the '870 Patent, despite F5's knowledge and understanding that F5's products and services infringe these patents. Thus, F5's infringement of '870 Patent is willful and egregious, warranting enhancement of damages.

227. As such, F5 has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously 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.

SECOND CAUSE OF ACTION

(F5's Indirect Infringement of the '870 Patent pursuant to 35 U.S.C. § 271(b))

228. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

229. As set forth above, F5 is liable for indirect infringement under 35 U.S.C. § 271(b) of at least Claims 1-20 and 37-38 of the '870 Patent at least as early as November 26, 2013, when Dr. Ford reached out to Ted Schlein, or no later than January 14, 2020, when SunStone's counsel sent Shape the Notice Letter, 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.

230. Since at least as early as November 26, 2013, but not later than January 14, 2020, F5, either alone or through Shape, has had knowledge of the '870 Patent. Since that time, F5 has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including F5's customers, to use the Accused Products in a manner that infringe the '870 Patent. This is evident when F5 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.

231. F5 specifically intends the Accused Products to be used and operated to infringe one or more claims, including at least Claims 1-20 and 37-38, of the '870 Patent.

232. F5 encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

233. As detailed above, F5 has instructed its customers to use the accused methods and Accused Products in an infringing manner.

234. F5's analysis and knowledge of the '870 Patent combined with its ongoing activity demonstrates F5's knowledge and intent that the identified features of its Accused Products be used to infringe the '870 Patent.

235. F5's knowledge of the '870 Patent and SunStone's infringement allegations against F5 combined with its knowledge of the Accused Products and how they are used to infringe the '870 Patent, consistent with F5's promotions and instructions, demonstrate F5's specific intent to induce users of the Accused Products to infringe the '870 Patent.

236. As set forth in paragraphs 163-183, F5 knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with F5, one or more method claims of the '870 Patent.

237. SunStone is entitled to recover from F5 compensation in the form of monetary damages suffered as a result of F5's infringement in an amount that cannot be less than a reasonable royalty together with interest and costs as fixed by this Court.

THIRD CAUSE OF ACTION

(F5's Direct Infringement of the '759 Patent pursuant to 35 U.S.C. § 271(a))

238. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

239. F5 has infringed and continues to infringe at least Claims 1-22 of the '759 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 Accused Product

that fall within the scope of one or more claims of the '759 Patent in violation of at least 35 U.S.C. § 271(a).

240. F5's infringing Accused Products include, without limitation, Shape Connect, ShapeShifter Elements, Shape Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and Silverline Shape Defense and other solutions with the same or similar features and functionality that satisfy each element of one or more asserted claims. Each of the above-referenced Accused Products incorporates or builds upon Shape Defense.

241. F5'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.

242. The Accused Products embody the patented invention of the '759 Patent and infringe the '759 Patent because they practice an apparatus comprising:

a security processor configured to:

receive, from a transaction server, i) hard information to transmit to a client device related to a transaction with the client device, the hard information including at least one of a) a data field in a webpage for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage that provides information related to the transaction, and ii) soft information including a first set of program code for the webpage that specifies how the hard information is to be displayed on the client device;

determine a variation of the soft information configured to prevent a malicious application from identifying the transaction with the client device, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed on the client device;

responsive to determining the variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the second set of program code;

responsive to determining that the variation of the soft information changes how the hard information is displayed, determine a second variation of the soft information configured to prevent a malicious application from identifying the transaction

with the client device, the second variation of the soft information including a third set of program code that specifies how the hard information is to be displayed on the client device;

responsive to determining the second variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the third set of program code; and transmit at least one message to the client device including the hard information and the variation of the soft information or the second variation of the soft information.

'759 Patent, Claim 15.

243. According to F5 and historical Shape documentation, the Accused Products utilize the Shape Defense platform. The documentation shows that the Accused Products have a security processor. For example, ShapeShifter Elements utilizes a security server, functioning as a Shape Botwall Service, located between the web server and the client user. Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021). Prior to being launched as ShapeShifter Elements, the product was known as PolyRef and was presented in a technical paper as early as June 2014. Ex. 50, Xinran Wang, et al., Polymorphism as a Defense for Automated Attack of Websites at 513–530 (Springer International Publishing, Switzerland 2014).

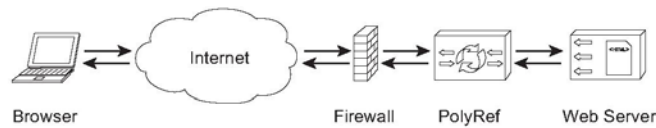
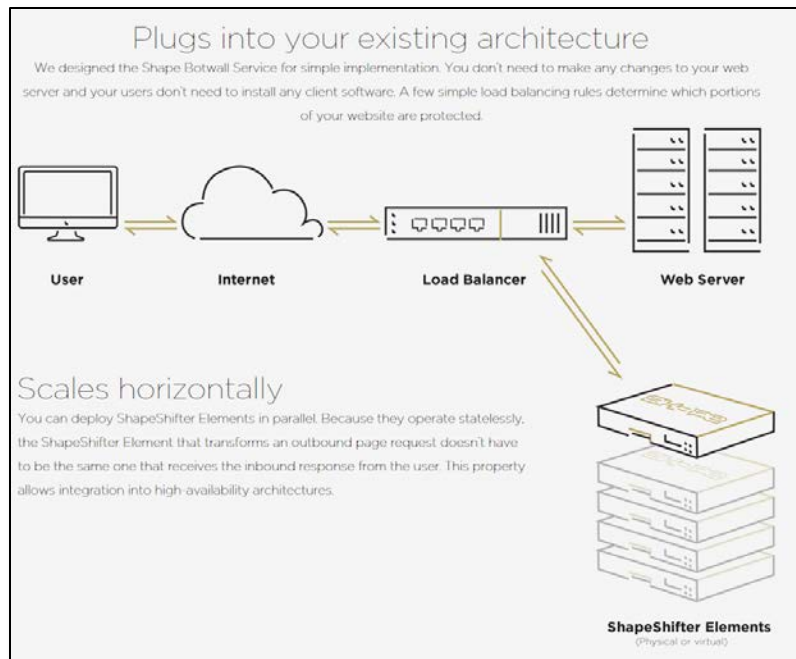



Fig. 1. PolyRef as a transparent proxy


Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021); Ex. 50, Xinran Wang, et al., Polymorphism as a Defense for Automated Attack of Websites at 513–530 (Springer International Publishing, Switzerland 2014).

244. F5 now refers to ShapeShifter Elements as Shape Defense, which includes the functionality of ShapeShifter Elements. Shape Defense offers greater coverage and tracking but still focuses on preventing sophisticated bot attacks on key web pages. The key web pages protected include login and checkout but cover other key pages so that Shape Defense can prevent bots from Account Takeover, Carding, Inventory Hoarding, Scraping, Gift Card Attacks and Marketing Fraud.



Shape Defense™


AI-POWERED WEB AND MOBILE FRAUD PREVENTION
FOR ORGANIZATIONS OF ALL SIZES



ATTACKS ON WEBSITES AND MOBILE APPS DRIVE FRAUD, RISK, AND BAD CUSTOMER EXPERIENCES

Every day, web and mobile applications face an onslaught of sophisticated attacks with one commonality: instead of exploiting application vulnerabilities, attackers abuse an application's functionality as it was intended for legitimate users. These imitation attacks - delivered by bots and other forms of automation - simulate human behavior using highly sophisticated attack tools, with the goal of conducting crime or disrupting business.

Shape Defense protects online businesses from such sophisticated attacks that would otherwise result in large scale fraud. Companies get the visibility, detection and mitigation outcomes they need to slash fraud, reduce cloud hosting, bandwidth and compute costs, improve user experiences, and optimize their business based on real human traffic.



WORLD-CLASS PROTECTION

Designed to meet the needs of a broad range of organizations, Shape Defense delivers world-class application protection that leverages the power of the Shape network.

AI-powered: Through the use of advanced AI and ML, Shape Defense accurately determines in real-time if an application request is from a fraudulent source and when it is, mitigates, while allowing legitimate human users without introducing additional friction.

Collective defense: Shape Defense customers benefit from everything Shape learns through the large protection network we operate. Every 24 hours, Shape blocks more than one billion fraudulent log-in attempts and other transactions, while ensuring that more than 150 million legitimate human transactions are kept safe.

Omnichannel protection: Shape Defense can be deployed to protect web and mobile applications, as well as HTTP APIs. The company's mobile SDK is deployed on more than 200 million iOS and Android devices worldwide.

Easy to deploy and flexible to implement: Shape Defense can be implemented in a variety of modes, including deployments as quick as 30 minutes, to suit the needs of the organization and to best mitigate any attack traffic the business experiences. And Shape Defense is managed through simplified administration that does not tax your security team to operate.

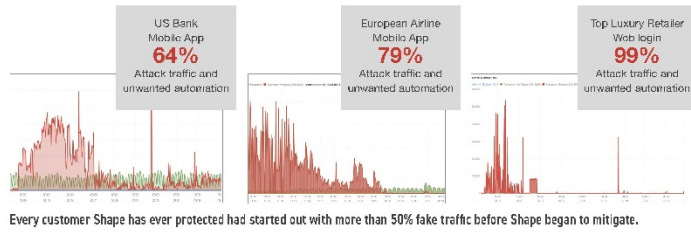
PROTECTION AGAINST BOTS AND OTHER AUTOMATION ATTACKS

Shape Defense protects against the most sophisticated credential stuffing, account take over attacks, carding, and the rest of the OWASP Automated Threats to Web Applications list. Shape Defense delivers continuous protection even when attackers retool, ensuring durable protection is sustained.

<p>Account Takeover</p> <p style="font-size: 0.7em; margin: 2px 0;">Stop fraudsters from rapidly testing stolen credentials on your login applications, which means they can't take over accounts in the first place.</p>	<p>Carding</p> <p style="font-size: 0.7em; margin: 2px 0;">Prevent criminals from using your checkout pages to validate stolen credit cards.</p>	<p>Scraping</p> <p style="font-size: 0.7em; margin: 2px 0;">Control how scrapers and aggregators harvest data from your website, allowing you to protect sensitive data and manage infrastructure costs.</p>
<p>Inventory Hoarding</p> <p style="font-size: 0.7em; margin: 2px 0;">Ensure your campaigns and most in-demand items are sold directly to your customers, not to scalpers.</p>	<p>Gift Card Attacks</p> <p style="font-size: 0.7em; margin: 2px 0;">Ensure gift card value, loyalty points and other stored value remains in your customers' hands.</p>	<p>Marketing Fraud</p> <p style="font-size: 0.7em; margin: 2px 0;">Ensure your business analytics and marketing spend are driven by real human users and not automated bots.</p>

shapesecurity.com sales@shapesecurity.com +1 (855) 399-0400

83

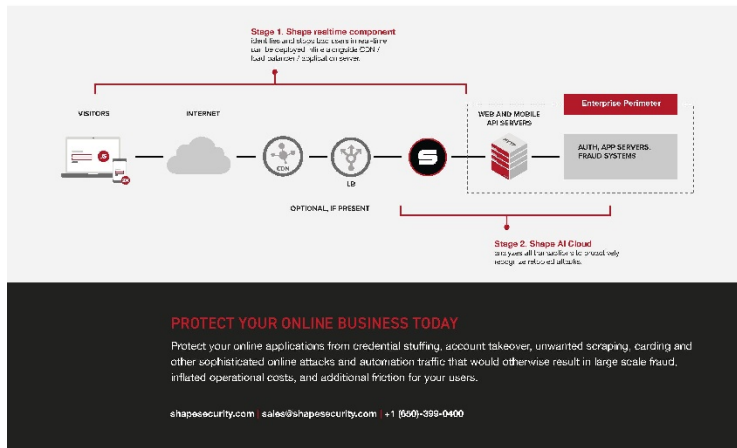


HOW SHAPE DEFENSE WORKS

Shape Defense uses a patented two-stage process to deliver highly accurate real-time detection and mitigation, as well as to provide sustained protection through attacker rotation.

Stage 1 evaluates each transaction across a set of proprietary risk factors that include network, activity, user, device and account factors. These risk factors are evaluated in light of everything Shape has learned across its global customer base. Shape's innovative Stage 1 sees all traffic - including mitigated automation traffic - and also includes insights learned from detecting fraudulent activity across other Shape clients (aggregated defense from aggregated insights).

Shape's unique Stage 2 defense counters the attackers' evolution with an after-action machine learning and human analysis. Specifically, our Stage 2 defensive system leverages three tiers of supervised and unsupervised learning and provides unparalleled protection. Shape AI Cloud analyzes all transactions to proactively recognize rotation attacks.



Ex. 23, 2020 Shape Defense Datasheet, available at <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

245. According to F5 and historical Shape documentation, the Accused Product have a security processor that is configured to receive, from a transaction server, i) hard information to transmit to a client device related to a transaction with the client device, the hard information including at least one of a) a data field in a webpage for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage that provides information related to the transaction, and ii) soft information including a first set of program code for the webpage that specifies how the hard information is to be displayed on the

client device. For example, in ShapeShifter Elements, the transactional server sends the transactional information to the security server. transactional information includes at least the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login. The ShapeShifter Elements can be a virtual server being functionally provided through software implementation rather than a physical device (i.e., SAAS). The security server also receives presentation information used to display and interact with the transactional information on the web page. The presentation information includes at least soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. *See* Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

246. As shown in the F5 and historical Shape documentation, the soft information coding is identified that a bot might search and then discover the type of information that is being requested so that the bot can respond with stolen usernames and passwords. The presentation information is described, in part, by specifying the explicit form “login_form.php” and the explicit variables needed for the form - “username” and “password.” A combination of presentation and transaction information that is an indication of the data fields and data/text requested to be displayed to acquire a password and a user ID / username (transaction or hard information).

An example countermeasure:
reference polymorphism

How do you change the very nature of HTML, to introduce a new security model, while still delivering open markup code to web browsers? Shape transforms pages in real-time to introduce polymorphic code which presents barriers which are difficult or impossible for attackers to overcome. Here's one simple example of code before and after being protected by the Shape Botwall Service:

ORIGINAL WEBSITE CODE (BEFORE)	TRANSFORMED WEBSITE CODE (AFTER)
<pre><form action="login_form.php"> <input id="username" name="username"/> <input id="password" name="password"/> <input type="submit"/> </form></pre> <p style="text-align: right; font-size: small;">Simplified HTML</p>	<pre><form action="R6bYEc2taB4e"> <input id="bNoeTn2bjf2F" name="p5TbGSGCf63g"/> <input id="k5Kb5jCT6p4t" name="yWTg3L082t2f"/> <input type="submit"/> </form></pre>

Id.

247. According to F5 and historical Shape documentation, the Accused Product have a security processor that is configured to determine a variation of the soft information configured to prevent a malicious application from identifying the transaction with the client device, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed on the client device. For example, the first set of program code is transformed to obscure the actual form (display information) used and the form entries requested. For example, the original form requested was “login_form.php” and is now replaced by the text “R6bYEc2taB4e”. A transformation table is kept in the security processor to inverse transform back to the necessary labels for the web server. *Id.*

248. According to F5 and historical Shape documentation, the Accused Product have a security processor that is configured to responsive to determining the variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the second set of program code. For example, the proposed first variation of the soft information (second set of program code). The quality control process is integral to the any modification process as part of best practices. The first variation of the soft information obscures

content from malicious bots (its purpose) but must not break the functionality of the webpage. The consequences of breaking functionality is that information will not be rendered and displayed properly, or perhaps not rendered at all, JavaScript will not run, and clicks will not function, and the entire web page might not even load. In such an instance, the first set of program code is replaced with the second set of program code if the quality control process verifies the functionality. *Id.*

249. According to F5 and historical Shape documentation, the Accused Product have a security processor that is configured to responsive to determining that the variation of the soft information changes how the hard information is displayed, determine a second variation of the soft information configured to prevent a malicious application from identifying the transaction with the client device, the second variation of the soft information including a third set of program code that specifies how the hard information is to be displayed on the client device. For example, the quality control process for website development includes remediation. If the first variation of soft information breaks the functionality of the webpage, a second variation of soft information must be developed, producing a third set of program code. Thereafter, a second variation of soft information is developed, and a third set of comparable program code remains. *Id.*

250. According to F5 and historical Shape documentation, the Accused Product have a security processor that is configured to responsive to determining the second variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the third set of program code; and transmit at least one message to the client device including the hard information and the variation of the soft information or the second variation of the soft information. For example, at this point, there is now a second variation of the soft

information (third set of program code). The iteration and quality control process further includes additional remediation. The second variation of the soft information obscures content from malicious bots (its purpose) but must not break the functionality of the webpage. The consequences of breaking functionality is that information will not be rendered and displayed properly, or perhaps not rendered at all, JavaScript will not run, and clicks will not function, and the entire web page might not even load. The third set of program code is quality control tested and modified until it is found to be compatible (iterations). *Id.*

251. The Accused Products satisfy each and every element of each asserted claim of the '759 Patent either literally or under the doctrine of equivalents.

252. As a result of F5'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.

253. F5's infringement of the '759 Patent has injured and continues to injure SunStone in an amount to be proven at trial.

254. As set forth in paragraphs 163-183, F5 has willfully infringed the '759 Patent. SunStone is informed and believes that F5, either alone or through Shape, had knowledge of the '759 Patent through various channels and despite its knowledge of SunStone's patent rights, engaged in egregious behavior warranting enhanced damages.

255. SunStone is informed and believes that despite F5 and Shape's knowledge of the '759 Patent and SunStone's patented technology, F5 and Shape made the deliberate decision(s) to sell products and services that each knew infringe SunStone's '759 Patent.

256. SunStone is informed and believes that F5 knew or was willfully blind to SunStone's technology and the '759 Patent. Despite this knowledge and/or willful blindness, F5

has acted with blatant and egregious disregard for SunStone's patent rights with an objectively high likelihood of infringement.

257. SunStone is informed and believes that F5 has undertaken no efforts to avoid infringement of the '759 Patent, despite F5's knowledge and understanding that F5's products and services infringe these patents. Thus, F5's infringement of '759 Patent is willful and egregious, warranting enhancement of damages.

258. As such, F5 has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously engage in acts of infringement of the '759 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.

FOURTH CAUSE OF ACTION

(F5's Indirect Infringement of the '759 Patent pursuant to 35 U.S.C. § 271(b))

259. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

260. As set forth above, F5 is liable for indirect infringement under 35 U.S.C. § 271(b) of at least Claims 1-22 of the '759 Patent at least as early as November 26, 2013, when Dr. Ford reached out to Ted Schlein, or no later than January 14, 2020, when SunStone's counsel sent Shape the Notice Letter, 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 '759 Patent.

261. Since at least as early as November 26, 2013, but not later than January 14, 2020, F5, either alone or through Shape, has had knowledge of the '759 Patent. Since that time, F5 has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including F5's customers, to use the Accused Products in a manner that infringe

the '759 Patent. This is evident when F5 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.

262. F5 specifically intends the Accused Products to be used and operated to infringe one or more claims, including at least Claims 1-22 of the '759 Patent.

263. F5 encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

264. As detailed above, F5 has instructed its customers to use the accused methods and Accused Products in an infringing manner.

265. F5's analysis and knowledge of the '759 Patent combined with its ongoing activity demonstrates F5's knowledge and intent that the identified features of its Accused Products be used to infringe the '759 Patent.

266. F5's knowledge of the '759 Patent and SunStone's infringement allegations against F5 combined with its knowledge of the Accused Products and how they are used to infringe the '759 Patent, consistent with F5's promotions and instructions, demonstrate F5's specific intent to induce users of the Accused Products to infringe the '759 Patent.

267. As set forth in paragraphs 163-183, F5 knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with F5, one or more of the asserted claims of the '759 Patent.

268. SunStone is entitled to recover from F5 compensation in the form of monetary damages suffered as a result of F5's infringement in an amount that cannot be less than a reasonable royalty together with interest and costs as fixed by this Court.

FIFTH CAUSE OF ACTION
(F5's Direct Infringement of the '537 Application
[U.S. Patent No. 10, __, __] pursuant to 35 U.S.C. § 271(a))

269. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

270. F5 has infringed and continues to infringe at least allowed and renumbered Claims 1-9 and 21-30 of the '537 Application 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 Accused Product that fall within the scope of one or more claims of the '537 Application in violation of at least 35 U.S.C. § 271(a).

271. F5's infringing Accused Products include, without limitation, Shape Connect, ShapeShifter Elements, Shape Defense, Shape Enterprise Defense, Shape AI Fraud Engine, and Silverline Shape Defense and other solutions with the same or similar features and functionality that satisfy each element of one or more asserted claims. Each of the above-referenced Accused Products incorporates or builds upon Shape Defense.

272. F5'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.

273. The Accused Products embody the patented invention of the '537 Application and infringe the '537 Application because they practice 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 a label of the presentation information,

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

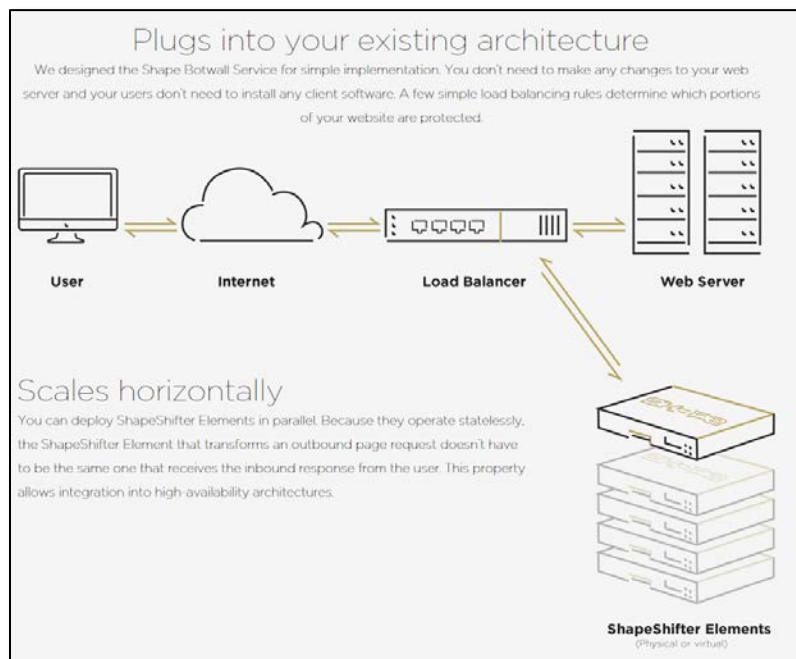
wherein the transactional information includes at least one of text, data, pictorial information, image information, information requested by the server to perform a service for the client device, authentication information, refinement information on a type of service requested by the client device,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

'537 Application, Claim [10].

274. According to F5 and historical Shape documentation, the Accused Products utilize the Shape Defense platform. As shown by historical Shape documentation, the Accused Products perform a method via a processor. For example, ShapeShifter Elements performs a method using a security server, functioning as a Shape Botwall Service, located between the web server and the client user. Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last

visited Jan. 21, 2021). Prior to being launched as ShapeShifter Elements, the product was known as PolyRef and was presented in a technical paper as early as June 2014. Ex. 50, Xinran Wang, et al., Polymorphism as a Defense for Automated Attack of Websites at 513–530 (Springer International Publishing, Switzerland 2014).

275. The Accused Products select, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device. For example, the transactional server sends the transactional information to the security server. Transactional information is the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login. In this configuration, the ShapeShifter Elements can be a virtual server (determined in discovery) being functionally provided through software implementation rather than a physical device (i.e., SAAS).



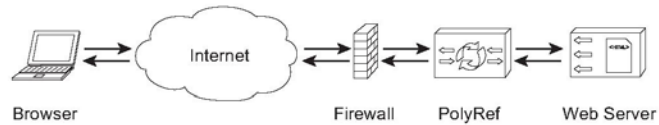
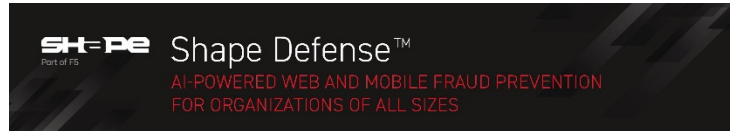


Fig. 1. PolyRef as a transparent proxy

Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 15, 2021); Ex. 50, Xinran Wang, et al., *Polymorphism as a Defense for Automated Attack of Websites* at 513–530 (Springer International Publishing, Switzerland 2014).

276. F5 now refers to ShapeShifter Elements as Shape Defense, which includes the functionality of ShapeShifter Elements. Shape Defense offers greater coverage and tracking but still focuses on preventing sophisticated bot attacks on key web pages. The key web pages protected include login and checkout but cover other key pages so that Shape Defense can prevent bots from Account Takeover, Carding, Inventory Hoarding, Scraping, Gift Card Attacks and Marketing Fraud.



ATTACKS ON WEBSITES AND MOBILE APPS DRIVE FRAUD, RISK, AND BAD CUSTOMER EXPERIENCES

Every day, web and mobile applications face an onslaught of sophisticated attacks with one commonality: instead of exploiting application vulnerabilities, attackers abuse an application's functionality as it was intended for legitimate users. These imitation attacks - delivered by bots and other forms of automation - simulate human behavior using highly sophisticated attack tools, with the goal of conducting crime or disrupting business.

Shape Defense protects online businesses from such sophisticated attacks that would otherwise result in large scale fraud. Companies get the visibility, detection and mitigation outcomes they need to slash fraud, reduce cloud hosting, bandwidth and compute costs, improve user experiences, and optimize their business based on real human traffic.



WORLD-CLASS PROTECTION

Designed to meet the needs of a broad range of organizations, Shape Defense delivers world-class application protection that leverages the power of the Shape network.

AI-powered: Through the use of advanced AI and ML, Shape Defense accurately determines in real-time if an application request is from a fraudulent source and when it is, mitigates, while allowing legitimate human users without introducing additional friction.

Collective defense: Shape Defense customers benefit from everything Shape learns through the large protection network we operate. Every 24 hours, Shape blocks more than one billion fraudulent log-in attempts and other transactions, while ensuring that more than 150 million legitimate human transactions are kept safe.

Omnichannel protection: Shape Defense can be deployed to protect web and mobile applications, as well as HTTP APIs. The company's mobile SDK is deployed on more than 200 million iOS and Android devices worldwide.

Easy to deploy and flexible to implement: Shape Defense can be implemented in a variety of modes, including deployments as quick as 30 minutes, to suit the needs of the organization and to best mitigate any attack traffic the business experiences. And Shape Defense is managed through simplified administration that does not tax your security team to operate.

PROTECTION AGAINST BOTS AND OTHER AUTOMATION ATTACKS

Shape Defense protects against the most sophisticated credential stuffing, account take over attacks, carding, and the rest of the OWASP Automated Threats to Web Applications list. Shape Defense delivers continuous protection even when attackers retool, ensuring durable protection is sustained.

Account Takeover

Stop fraudsters from rapidly testing stolen credentials on your login applications, which means they can't take over accounts in the first place.

Inventory Hoarding

Ensure your campaigns and most in-demand items are sold directly to your customers, not to scalpers.

Gift Card Attacks

Ensure gift card value, loyalty points and other stored value remains in your customers' hands.

Carding

Prevent criminals from using your checkout pages to validate stolen credit cards.

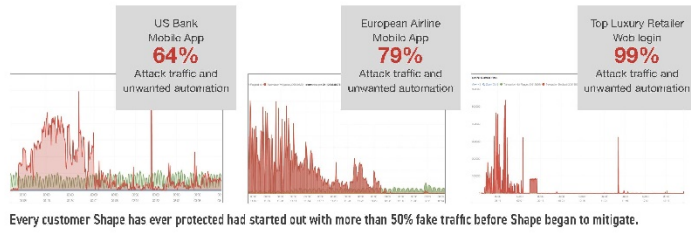
Scraping

Control how scrapers and aggregators harvest data from your website, allowing you to protect sensitive data and manage infrastructure costs.

Marketing Fraud

Ensure your business analytics and marketing spend are driven by real human users and not automated bots.

shapesecurity.com sales@shapesecurity.com +1 (505) 399-0400

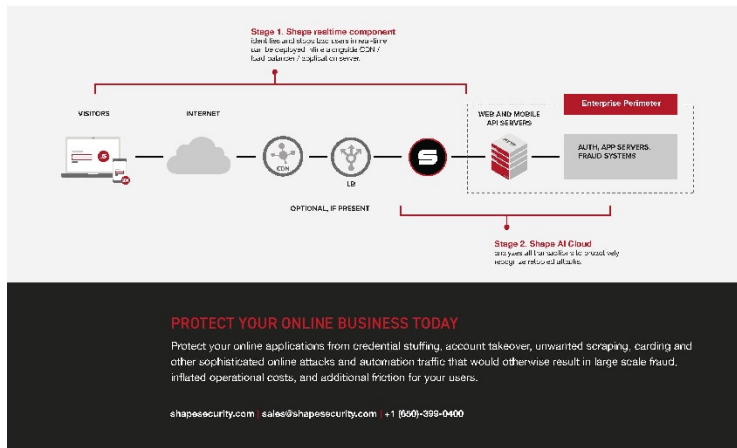


HOW SHAPE DEFENSE WORKS

Shape Defense uses a patented two-stage process to deliver highly accurate real-time detection and mitigation, as well as to provide sustained protection through attacker rotation.

Stage 1 evaluates each transaction across a set of proprietary risk factors that include network, activity, user, device and account factors. These risk factors are evaluated in light of everything Shape has learned across its global customer base. Shape's innovative Stage 1 sees all traffic - including mitigated automation traffic - and also includes insights learned from detecting fraudulent activity across other Shape clients (aggregated defense from aggregated insights).

Shape's unique Stage 2 defense counters the attackers' evolution with an after-action machine learning and human analysis. Specifically, our Stage 2 defensive system leverages three tiers of supervised and unsupervised learning and provides unparalleled protection. Shape AI Cloud analyzes all transactions to proactively recognize rotation attacks.



Ex. 23, 2020 Shape Defense Datasheet, available at <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

277. The Accused Products select 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. For example, the security server also receives presentation information used to display and interact with the transactional information on the web page. The presentation information includes at least soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. See Ex. 49, The

Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

278. The Accused Products transmit, via the processor, at least one message including the presentation and transactional information from the server to the client device. For example, the information sent from the F5 server to the client device includes the presentation information and transactional information. *See* Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021); Ex. 50, Xinran Wang, et al., *Polymorphism as a Defense for Automated Attack of Websites* at 513–530 (Springer International Publishing, Switzerland 2014). *See* Ex. 23, 2020 Shape Defense Datasheet, *available at* <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

279. The Accused Devices determine, 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. For example, the security server modifies the presentation information to obscure the existence of the transactional information from malicious code. Therefore, an acceptable response must be via the security server to recover the inverse transform. In addition, the type of client display is communicated to the web server as part of the request to visit the web page. The HTML presentation information code must be anchored to the display device and pixel locations become important. Finally, the transactional

information such as user ID / username and password must match the registered security information for the client. *Id.*

280. The Accused Products receive, in the processor, the response message from the client device and, responsive to information in the response message not matching the prediction, provide, via the processor, an indication there is a malicious application affecting communications between the server and the client device. For example, in the Accused Products a response message is detected and blocked from returning to the web server due to the presence of an unacceptable response detect when a response message contains code that does not logically follow (i.e., acceptable response) from the modified presentation information sent to the client. This type of response is considered an unacceptable response and indicates the presence of a malicious application (bot). For example, “bNoeTn2bjf2F” is the expected response for username. If a bot sent “username” instead of “bNoeTn2bjf2F”, the inverse transform via the security server would not know how to transform “username” since it is not listed in the reverse transform as a starting point. This inability to transform it back to web server recognizable code is an indication of malicious code (bot) being present and can be detected. *Id.*; Ex. 23, 2020 Shape Defense Datasheet, *available at* <https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape%20Defense%20-%20Product%20datasheet.pdf> (last visited Jan. 15, 2021) (annotations added).

281. In the Accused Devices, the prediction is further determined by the processor based at least in part by estimating a label of the presentation information. For example, in the Accused Products, the first set of website code is transformed to obscure the web server’s name for the form (presentation information) used and the form’s transactional information entries requested. For example, the original form requested was “login_form.php” and is now replaced by the text string “R6bYEc2taB4e”. A transformation table is kept in the security processor to inverse transform

back to the necessary labels for the web server. Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

282. In the Accused Devices, 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, in the Accused Products, the presentation information includes at least soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. Ex. 49, The Shape Botwall Service (Sept. 10, 2015), *available at* <https://web.archive.org/web/20150910182831/http://www.shapesecurity.com/product/> (last visited Jan. 21, 2021).

283. In the Accused Products, 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. For example, in the Accused Devices, transactional information includes at least the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login.

284. The Accused Products satisfy each and every element of each asserted claim of the '537 Application either literally or under the doctrine of equivalents.

285. F5's infringing activities are and have been without authority or license under the '537 Application.

286. SunStone is entitled to recover from F5 the damages sustained by SunStone as a result of F5's infringing acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

SIXTH CAUSE OF ACTION
(F5's Indirect Infringement of the '537 Application
[U.S. Patent No. 10, __, __] pursuant to 35 U.S.C. § 271(b))

287. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

288. As set forth above, F5 is liable for indirect infringement under 35 U.S.C. § 271(b) of at least Claims 1-9 and 21-30 of the '537 Application at least as early as service of the 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 '537 Application.

289. Since at least as early as service of this original Complaint, has had knowledge of the '537 Application. Since that time, F5 has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Products, including F5's customers, to use the Accused Products in a manner that infringe the '537 Application. This is evident when F5 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.

290. F5 specifically intends the Accused Products to be used and operated to infringe one or more claims, including at least Claims 1-9 and 21-30, of the '537 Application.

291. F5 encourages, directs, aids, and abets the use, configuration, and installation of the Accused Products.

292. As detailed above, F5 has instructed its customers to use the accused methods and Accused Products in an infringing manner.

293. F5's analysis and knowledge of the '537 Application combined with its ongoing activity demonstrates F5's knowledge and intent that the identified features of its Accused Products be used to infringe the '537 Application.

294. F5's knowledge of the '537 Application and SunStone's infringement allegations against F5 combined with its knowledge of the Accused Products and how they are used to infringe the '537 Application, consistent with F5's promotions and instructions, demonstrate F5's specific intent to induce users of the Accused Products to infringe the '537 Application.

295. SunStone is entitled to recover from F5 compensation in the form of monetary damages suffered as a result of F5's infringement in an amount that cannot be less than a reasonable royalty together with interest and costs as fixed by this Court.

SEVENTH CAUST OF ACTION
(Capital One's Direct Infringement of the '870 Patent pursuant to 35 U.S.C. § 271(a))

296. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

297. Capital One has infringed and continues to infringe at least Claims 1-20 and 37-38 of the '870 Patent by, among other things, making, using, selling, testing, performing methods, and/or offering for sale in the United States—without license or authority—including its own use

and testing of, products, devices, or systems, including the Accused Capital One Products and Services 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).

298. Capital One's accused products and services include the Capital One website and servers, which utilizes at least certain functions of the Shape Defense product in conjunction with Capital One's servers, source code, personnel, and customers (the "Accused Capital One Products and Services").

299. Capital One's acts of making, using, selling, and/or offering for sale accused products and services have been without the permission, consent, authorization, or license of SunStone.

300. The Accused Capital One Products and Services embody the patented invention of the '870 Patent and infringe the '870 Patent because they practice 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.

301. The Accused Capital One Products and Services utilize the Shape Defense software in conjunction with Capital One's own website, products, and services. The Capital One website is stored on servers operated by or belonging to Capital One. The interaction with the Capital One website occurs on behalf of Capital One customer devices or client devices. The webpage source code of the Capital One website was developed by or at the direction of Capital One.

```
function X(y) {var l=[],q=1;var j=ReferenceError, k=TypeError, B=Object, g=RegExp, S=Number, I=String, e=Array, c=R.bind, a=R.call, z=S.bind(c, a), F=R.apply, K=Date, F=[].push, L=[].pop, E=[].slice, S=[].splice, W=[].join, D=[].map, T=Date, C=Date, R=Date, n=Date, O=Date;
;(function(e) {e.initCustomEvent("Ke8fNVikq", false, false, ["A0UodSh2AOAAinsPUo07D64rANaeo1h9pccGVo34AY_m-l18KFFJNFjw9TszAWw4N-SuhuewH0AAEBJAAMAAA==", "Fdp=hLs9cK05kUYya40MPxq_ERXVV82-3tn78csm]woWG21IQuFuM16dCOAhefgz1"];
[[], [1264226299, 650393125, 1219289424, 1229708843, 320189661, 1379240126, 1335093598, 1643315645], "okUq3Ft5n79rFXyBh/077QKR", "okUq3Ft5n79rFXyBh/077QKR", [], typeOf: arguments="undefined", void: 0; arguments[]]; dispatchEvent(a); (document.createEvent("CustomEvent"))});
```

Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

302. The Accused Capital One Products and Services select transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device. For example, when a Capital One customer device or client device visits the Capital One sign in webpage at <https://verified.capitalone.com/auth/signin>, the Capital One webpage transmits transactional information from a Capital One server to the Capital One customer device or client device's device based on the request from the Capital One customer device or client device's device. Transactional information is the coding and variables on the Capital One

webpage, such as a user ID / username or password, that is essential to completing the transaction such as a login.

The screenshot displays the Capital One Customer Sign In Webpage in a browser. The webpage shows a sign-in form with fields for Username (JohnSmith) and Password (masked with dots), a 'Remember Me' checkbox, and a 'Sign In' button. Below the form are links for 'Forgot Username or Password?' and 'Set Up Online Access'. At the bottom, there are links for 'Looking for these accounts? Business or Commercial'. The browser's developer tool is open, showing a list of network requests. The 'Network' tab is active, displaying a table of requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The first request is a GET request to 'verified...cp_common.js' with a status of 200. Other requests include 'verified...smartBanner.js', 'verified...bfp-ah-min.js', 'runtime-39966deed9a7221223e.js', 'polyfill.a6a90bfad418966a30.js', 'scripts.2261e7ce9447b0a0575b.js', 'main.029add6ef8fc2270b5f0.js', 'js-a...nr-spa-1169-min.js', 'tmx.cap...Bootstrap.js', 'bfp.cac...browserFingerPrintV1.min.js', 'verified...uba.js', 'verified...web_properties.js', 'devices...ccjs?tid=slc_0145b1ea-7a40-4472', 'tmx.cap...serverComponent.php?m=5715628', 'w.usabl...45796c56d2a3.js?m=1', 'suc.cdn...6.js?namespace=cotdip', 'tmx.cap...9904715922288e8b3115da796a0', 'tmx.cap...0eb5b22ec0871a30013d83548ef', 'tmx.cap...e0646c2ceaf1e04a25a5830cc97e', and 'bam...c344d5e907a=7956961910aa=10'. The right-hand pane of the developer tool shows the 'Response Headers' for the selected request, including 'Cache-Control: no-cache, no-store, must-revalidate', 'Connection: keep-alive', 'Content-Encoding: gzip', 'Content-Type: Application/javascript, charset=UTF-8', 'Date: Wed, 06 Jan 2021 16:10:24 GMT', 'Expires: Wed, 06 Jan 2021 16:10:24 GMT', 'Pragma: no-cache', 'Transfer-Encoding: chunked', 'Vary: Accept-Encoding', and 'X-Ion-Msg: prod'. The 'Request Headers' pane shows 'Accept: */*', 'Accept-Encoding: gzip, deflate, br', 'Accept-Language: en-US,en;q=0.5', 'Cache-Control: max-age=0', 'Connection: keep-alive', 'Cookie: TELID=353EBC0D9D428E8D0847E2A8EC3EE4; AMCV_317906C354252889...', and 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4398.90 Safari/537.36'.

Capital One Customer Sign In Webpage, available at <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

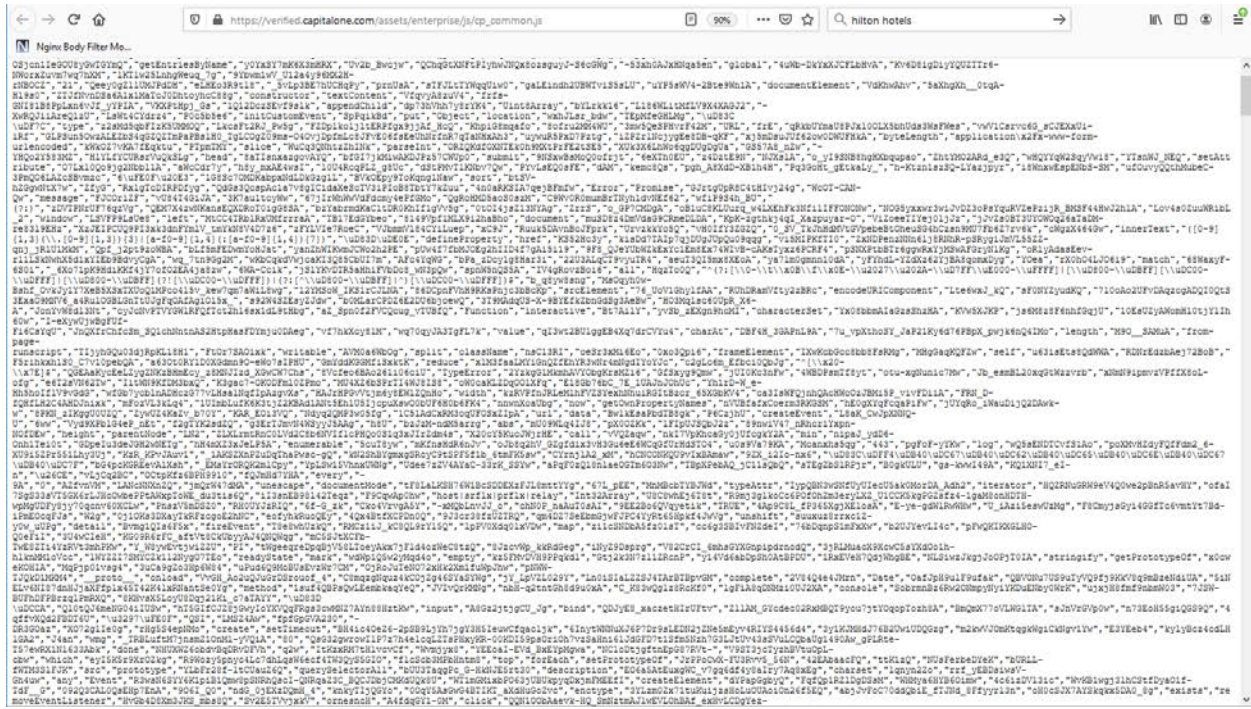
303. The Accused Capital One Products and Services select presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. For example, the Capital One server receives presentational information corresponding to the transactional information. The presentation information is used to display and interact with the transactional information on the web page of the Capital One customer device or client device. *Id.*

304. The Accused Capital One Products and Services transmit at least one message including the presentation and transactional information from the server to the client device. A message from the Capital One server is sent containing presentation and transactional information,

the message is further sent to at least the F5 server. The message received by the Capital One customer device or client device further includes at least the presentation information and transactional information.

305. The Accused Capital One Products and Services determine 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. For example, information is sent to at least the F5 server from the Capital One servers based on the Capital One customer device or client device. The F5 server modifies the presentation information to obscure the existence of the transactional information from malicious code. The modified code is sent back to the Capital One server. A review of source website code for the corporate website of Capital One demonstrate that the website obfuscates the source code constantly, to prevent automated attacks. The Java Script code shows that Capital One changes the source code constantly, to prevent automated attacks. An acceptable response must be via the server to recover the inverse transform or additional code. Moreover, Capital One's website includes source code stored on Capital One servers that discerns the type of display utilized by the Capital One customer device or client device, which is communicated to the Capital One web server and the F5 web server as part of the request by the Capital One customer device or client device to visit the Capital One webpage. The HTML presentation information code stored on the Capital One webserver must be anchored to the Capital One customer device or client device display device and pixel locations become important. This code developed by Capital One and shared with F5 as part of the Accused Capital One Products and Services is integral in the Capital One implementation. The transactional information such as

user ID / username and password of the Capital One customer device or client device, and as programmed on the Capital One webpage, must match the registered security information for the client.



Capital One Customer Sign In Webpage, available at <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

306. The Accused Capital One Products and Services receive the response message from the client device. For example, the Capital One servers receive the response message from the Capital One customer device or client device.

307. The Accused Capital One Products and Services responsive to information in the response message not matching the expected data, provide an indication there is a malicious application affecting communications between the server and the client device. For example, in the Accused Capital One Products and Services a response message is detected and blocked from returning to the Capital One web server due to the presence of an unacceptable response detect

when a response message contains code that does not logically follow (i.e., acceptable response) from the modified presentation information sent to the Capital One customer device or client device. This type of response is considered an unacceptable response and indicates the presence of a malicious application (bot), rather than a Capital One customer device or client device. The scrambled data is based on an interaction between the Capital One website and the F5 server, with source code from both Capital One and F5 required to complete the method.

308. In the Accused Capital One Products and Services the acceptable response is further determined by estimating a label of the presentation information, estimating a utilization of a codeword set based on the presentation information and transactional information, and/or estimating a utilization of a codeword set based on actions taken by at least one of the Capital One customer and the client device. For example, the Capital One webpage includes alterations in the website source code. In the Accused Capital One Products and Services, the acceptable response is further determined by estimating locations of rendered features and functions as displayed by the client device, estimating locations of rendered page geometry of the features and functions, and estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device. *Id.*

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

310. As a result of Capital One'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.

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

312. As set forth in paragraphs 196-200, Capital One has willfully infringed the '870 Patent. SunStone is informed and believes that Capital One had knowledge of the '870 Patent through various channels and despite its knowledge of SunStone's patent rights, engaged in egregious behavior warranting enhanced damages.

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

314. SunStone is informed and believes that Capital One knew or was willfully blind to SunStone's technology and the '870 Patent. Despite this knowledge and/or willful blindness, Capital One has acted with blatant and egregious disregard for SunStone's patent rights with an objectively high likelihood of infringement.

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

316. As such, Capital One has acted and continues to act recklessly, willfully, wantonly, deliberately, and egregiously 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.

EIGHTH CAUSE OF ACTION
**(Capital One's Indirect Infringement of the '870 Patent
pursuant to 35 U.S.C. § 271(b))**

317. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

318. As set forth above, Capital One is liable for indirect infringement under 35 U.S.C. § 271(b) of at least Claims 1-20 and 37-38 of the '870 Patent at least as early as May 2015, when a SunStone representative reached out to Capital One, because it knowingly encourages, aids, and directs others (*e.g.*, end users and customers) to use and operate the Accused Capital One Products and Services in an infringing manner and to perform the claimed methods of the '870 Patent.

319. Since at least as early as s May 2015, Capital One has had knowledge of the '870 Patent. Since that time, Capital One has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Capital One Products and Services, including Capital One's customers, to use the Accused Capital One Products and Services in a manner that infringe the '870 Patent. This is evident when Capital One encourages and instructs customers and other end users in the use and operation of the Accused Capital One Products and Services via advertisement, technical material, instructional material, and otherwise.

320. Capital One specifically intends the Accused Capital One Products and Services to be used and operated to infringe one or more claims, including at least Claims 1-20 and 37-38, of the '870 Patent.

321. Capital One encourages, directs, aids, and abets the use, configuration, and installation of the Accused Capital One Products and Services.

322. As detailed above, Capital One has instructed its customers to use the accused methods and Accused Capital One Products and Services in an infringing manner.

323. Capital One's analysis and knowledge of the '870 Patent combined with its ongoing activity demonstrates Capital One's knowledge and intent that the identified features of its Accused Capital One Products and Services be used to infringe the '870 Patent.

324. Capital One's knowledge of the '870 Patent and SunStone's infringement allegations against Capital One combined with its knowledge of the Accused Capital One Products and Services and how they are used to infringe the '870 Patent, consistent with Capital One's promotions and instructions, demonstrate Capital One's specific intent to induce users of the Accused Capital One Products and Services to infringe the '870 Patent.

325. As set forth in paragraphs 196-200, Capital One knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Capital One, one or more method claims of the '870 Patent.

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

NINTH CAUSE OF ACTION
**(Capital One's Direct Infringement of the '759 Patent
pursuant to 35 U.S.C. § 271(a))**

327. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

328. Capital One has infringed and continues to infringe at least Claims 1-22 of the '759 Patent by, among other things, making, using, selling, testing, performing methods, and/or offering for sale in the United States—without license or authority—including its own use and testing of, products, devices, or systems, including the Accused Capital One Products and Services that fall within the scope of one or more claims of the '759 Patent in violation of at least 35 U.S.C. § 271(a).

329. Capital One's infringing Accused Capital One Products and Services include the Capital One website, which utilizes at least certain functions of the Shape Defense product in conjunction with Capital One's servers, source code, personnel, and customers.

330. Capital One's acts of making, using, selling, and/or offering for sale accused products and services have been without the permission, consent, authorization, or license of SunStone.

331. The Accused Capital One Products and Services embody the patented invention of the '759 Patent and infringe the '759 Patent because they practice a method of varying soft information related to the display of hard information, the method comprising:

receiving in a security processor from a transaction server, i) the hard information to transmit to a client device within at least one message related to a transaction between the transaction server and the client device, the hard information including at least one of a) a data entry field in a webpage application for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage application that provides information related to the transaction, and ii) the soft information for transmission to the client device within the at least one message, the soft information including a first set of program code for the webpage application that specifies how the hard information is to be displayed within the webpage application on the client device;

determining, via the security processor, a variation of the soft information configured to prevent a malicious application from determining the transaction between the client device and the transaction server by at least identifying the hard information, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed within the webpage application on the client device;

determining, via the security processor, whether the variation of the soft information changes how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information;

responsive to determining the variation of the soft information does not change how the hard information is displayed, replacing the first set of program code with the second set of program code for the at least one message and transmitting, from the security processor to the client device, the at least one message including the hard information and the variation of the soft information;

information including at least one of a) a data entry field in a webpage application for a user of the client device to provide information associated with the transaction and b) text or data for display within the webpage application that provides information related to the transaction, and ii) the soft information for transmission to the client device within the at least one message, the soft information including a first set of program code for the webpage application that specifies how the hard information is to be displayed within the webpage application on the client device. The Accused Capital One Products and Services have a security processor. The Capital One website is housed on a webserver. In addition, the Shape Defense software is located between the web server and the client user. The Capital One website protects against malicious bot login. Information from the Capital One web server is sent and received based on interaction by a bot or Capital One customer device. Transactional information includes at least the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login. This coding was performed at least in part by Capital One or on behalf of Capital One. The security server also receives presentation information used to display and interact with the transactional information on the Capital One web page. The presentation information includes at least soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. Review of source website code for the Capital One website of Capital One demonstrate that the Capital One website obfuscates the source code constantly, to prevent automated attacks. The Java Script code shows that Capital One changes the source code constantly, to prevent automated attacks. An acceptable response must be via the server to recover the inverse transform or additional code. Moreover, Capital One's website includes source code stored on Capital One servers that discerns the type of display utilized by the

Capital One customer device or client device, which is communicated to the Capital One web server and the F5 web server as part of the request by the Capital One customer device or client device to visit the Capital One webpage. The HTML presentation information code stored on the Capital One webserver must be anchored to the Capital One customer device or client device display device and pixel locations become important. This code developed by Capital One and shared with F5 as part of the Accused Capital One Products and Services is integral in the Capital One implementation. The transactional information such as user ID / username and password of the Capital One customer device or client device, and as programmed on the Capital One webpage, must match the registered security information for the client.

The screenshot shows the Capital One Sign In webpage in a browser. The page has a "Sign In" heading, a "Username" field containing "JohnSmith", a "Password" field with masked characters, a "Remember Me" checkbox, and a green "Sign In" button. Below the button are links for "Forgot Username or Password?" and "Set Up Online Access". At the bottom, there is a section for "Looking for these accounts?" with a link for "Business or Commercial".

Overlaid on the right side of the browser is the developer tools network tab, showing a list of network requests. The selected request is a GET request for "cp_common.js" with a status of 200. The network tab also shows various headers and cookies for the selected request.

Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

334. The Accused Capital One Products and Services determine, via the security processor, a variation of the soft information configured to prevent a malicious application from

determining the transaction between the client device and the transaction server by at least identifying the hard information, the variation of the soft information including a second set of program code that specifies how the hard information is to be displayed within the webpage application on the client device. For example, the first set of program code as developed by Capital One is transformed to obscure the actual form (display information) used and the form entries requested. For example, the original form developed by Capital One is replaced by randomized or obscured text. A transformation table is kept on the Capital One and/or F5 security processor to inverse transform back to the necessary labels for the web server.

335. The Accused Capital One Products and Services determine, via the security processor, whether the variation of the soft information changes how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information. For example, the first set of program code as developed by Capital One is transformed to obscure the actual form (display information) used and the form entries requested. For example, the original form developed by Capital One is replaced by randomized or obscured text. A transformation table is kept on the Capital One and/or F5 security processor to inverse transform back to the necessary labels for the web server.

336. The Accused Capital One Products and Services, responsive to determining the variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the second set of program code for the at least one message and transmitting, from the security processor to the client device, the at least one message including the hard information and the variation of the soft information. For example, the proposed first variation of the soft information (second set of program code). The quality control process is integral to the any modification process as part of best practices. The first variation of the soft

information obscures content from malicious bots (its purpose) but must not break the functionality of the webpage. The consequences of breaking functionality is that information will not be rendered and displayed properly, or perhaps not rendered at all, JavaScript will not run, and clicks will not function, and the entire web page might not even load. In such an instance, the first set of program code is replaced with the second set of program code if the quality control process verifies the functionality. The quality control process is also integral to Capital One's website and development process in order to keep the Capital One website running for its customers.

337. The Accused Capital One Products and Services, responsive to determining that the variation of the soft information changes how the hard information is displayed at the client device, determine a second variation of the soft information configured to prevent a malicious application from determining the transaction between the client device and the transaction server, the second variation of the soft information including a third set of program code that specifies how the hard information is to be displayed within the webpage application on the client device. For example, the quality control process for website development includes remediation. If the first variation of soft information breaks the functionality of the webpage, a second variation of soft information must be developed, producing a third set of program code. Thereafter, a second variation of soft information is developed, and a third set of comparable program code remains. The quality control process is also integral to Capital One's website and development process in order to keep the Capital One website running for its customers.

338. The Accused Capital One Products and Services determine the second variation of the soft information does not change how the hard information is displayed at the client device compared to how the hard information was to be displayed using the soft information. For example, at this point, there is now a second variation of the soft information (third set of program

code). The iteration and quality control process further includes additional remediation. The second variation of the soft information obscures content from malicious bots (its purpose) but must not break the functionality of the webpage. The consequences of breaking functionality is that information will not be rendered and displayed properly, or perhaps not rendered at all, JavaScript will not run, and clicks will not function, and the entire web page might not even load. The third set of program code is quality control tested and modified until it is found to be compatible (iterations). The quality control process is also integral to Capital One's website and development process in order to keep the Capital One website running for its customers.

339. The Accused Capital One Products and Services, responsive to determining the second variation of the soft information does not change how the hard information is displayed, replace the first set of program code with the third set of program code for the at least one message and transmitting, from the security processor to the client device, the at least one message including the hard information and the second variation of the soft information. For example, at this point, there is now a second variation of the soft information (third set of program code). The iteration and quality control process further includes additional remediation. The second variation of the soft information obscures content from malicious bots (its purpose) but must not break the functionality of the webpage. The consequences of breaking functionality is that information will not be rendered and displayed properly, or perhaps not rendered at all, JavaScript will not run, and clicks will not function, and the entire web page might not even load. The third set of program code is quality control tested and modified until it is found to be compatible (iterations). The quality control process is also integral to Capital One's website and development process in order to keep the Capital One website running for its customers.

340. The Accused Capital One Products and Services satisfy each and every element of each asserted claim of the '759 Patent either literally or under the doctrine of equivalents.

341. Capital One's infringing activities are and have been without authority or license under the '759 Patent.

342. SunStone is entitled to recover from Capital One the damages sustained by SunStone as a result of Capital One's infringing acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

TENTH CAUSE OF ACTION
(Capital One's Indirect Infringement of the '759 Patent
pursuant to 35 U.S.C. § 271(b))

343. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

344. As set forth above, Capital One is liable for indirect infringement under 35 U.S.C. § 271(b) of at least Claims 1-22 of the '759 Patent at least as early as service of the Complaint because it knowingly encourages, aids, and directs others (e.g., end users and customers) to use and operate the Accused Capital One Products and Services in an infringing manner and to perform the claimed methods of the '537 Application.

345. Since at least as early as service of this original Complaint, has had knowledge of the '759 Patent. Since that time, Capital One has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Capital One Products and Services, including Capital One's customers, to use the Accused Capital One Products and Services in a manner that infringe the '537 Application. This is evident when Capital One encourages and instructs customers and other end users in the use and operation of the Accused

Capital One Products and Services via advertisement, technical material, instructional material, and otherwise.

346. Capital One specifically intends the Accused Capital One Products and Services to be used and operated to infringe one or more claims, including at least Claims 1-22 of the '759 Patent.

347. Capital One encourages, directs, aids, and abets the use, configuration, and installation of the Accused Capital One Products and Services.

348. As detailed above, Capital One has instructed its customers to use the accused methods and Accused Capital One Products and Services in an infringing manner.

349. Capital One's analysis and knowledge of the '759 Patent combined with its ongoing activity demonstrates Capital One's knowledge and intent that the identified features of its Accused Capital One Products and Services be used to infringe the '759 Patent.

350. Capital One's knowledge of the '759 Patent and SunStone's infringement allegations against Capital One combined with its knowledge of the Accused Capital One Products and Services and how they are used to infringe the '759 Patent, consistent with Capital One's promotions and instructions, demonstrate Capital One's specific intent to induce users of the Accused Capital One Products and Services to infringe the '759 Patent.

351. As set forth above, Capital One knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users or developers, to infringe by practicing, either themselves or in conjunction with Capital One, one or more of the asserted claims of the '759 Patent.

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

ELEVENTH CAUSE OF ACTION
(Capital One's Direct Infringement of the '537 Application
[U.S. Patent No. 10, __, __] pursuant to 35 U.S.C. § 271(a))

353. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

354. Capital One has infringed and continues to infringe at least Claims 1-9 and 21-30 of the '537 Application Patent by, among other things, making, using, selling, testing, performing methods, and/or offering for sale in the United States—without license or authority—including its own use and testing of, products, devices, or systems, including the Accused Capital One Products and Services that fall within the scope of one or more claims of the '537 Application in violation of at least 35 U.S.C. § 271(a).

355. Capital One's infringing Accused Capital One Products and Services include the Capital One website, which utilizes at least certain functions of the Shape Defense product in conjunction with Capital One's servers, source code, personnel, and customers.

356. Capital One's acts of making, using, selling, and/or offering for sale accused products and services have been without the permission, consent, authorization, or license of SunStone.

357. The Accused Capital One Products and Services embody the patented invention of the '537 Application and infringe the ' 537 Application because they practice 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.

'537 Application, Claim [1].

358. The Accused Capital One Products and Services utilize the Shape Defense software in conjunction with Capital One's own website, products, and services. The Capital One website is stored on servers operated by or belonging to Capital One. The interaction with the Capital One

website occurs on behalf of Capital One customer devices or client devices. The webpage source code of the Capital One website was developed by or at the direction of Capital One.

```
function X(y){var l=[];var O=ReferenceError;var TypeError=Object;var RegExp=Number;var String=Array;var bind=R.call;var bind(c,A).F=R.apply;var x=2;P.F=[].push;L=[].pop;F=[].slice;S  
;(function(e){e.initCustomEvent("EeBfNVikq",false,false,["A0U0d3h2ACAAInzP0o07D64zANae0h9pGcGVo34AY_m-1i8KFFJNFie9TszANva4N-  
cuIuewH9AAEB3AAAAA==", "Fbp-hLg9cK05kUYya4DNFkq_BPXvVB2-3tn78r2mjwoWz2110uF7M16dCOAHeTqzi", "1264226299,680393125,1219389424,1229708043,328189661,1579240126,1335093598,1649315645"], [1264226299,680393125,1219389424,1229708043,328189661,1579240126,1335093598,1649315645], "okUq3Ft5n79eFXybh/07QKK", "okUq3Ft5n79eFXybh/07QKK", {}, typeOf  
arguments=="undefined"?void 0:arguments});dispatchEvent(e)}(document.createEvent("CustomEvent"));
```

Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

359. The Accused Capital One Products and Services, select, via a processor, transactional information to transmit from a server to a communicatively coupled client device based on a request from the client device. For example, the Capital One website is stored on servers owned or operated by Capital One. For example, when a Capital One customer device or client device visits the Capital One sign in webpage at <https://verified.capitalone.com/auth/signin>, the Capital One webpage transmits transactional information from a Capital One server to the Capital One customer device or client device's device based on the request from the Capital One customer device or client device's device. Transactional information is the coding and variables on the Capital One webpage, such as a user ID / username or password, that is essential to completing the transaction such as a login.

The screenshot displays the Capital One sign-in page at <https://verified.capitalone.com/auth/signin>. The page features a "Sign In" form with fields for "Username" (containing "JohnSmith") and "Password" (masked with dots). A "Remember Me" checkbox is present, along with a green "Sign In" button. Below the button are links for "Forgot Username or Password?" and "Set Up Online Access". At the bottom, there is a section for "Looking for these accounts?" with a link for "Business or Commercial".

Overlaid on the right side of the page is a browser developer tool's Network tab. It shows a list of network requests, including:

- GET [verified...cp_common.js](#) (script, 96.45 KB)
- GET [verified...smartBanner.js](#) (script, 1.25 KB)
- GET [verified...bfp-ah-min.js](#) (script, 12.43 KB)
- GET [verified...runtime.59f66deed9a721223e.js](#) (script, 1.84 KB)
- GET [verified...polyfill.a6a90fa6da1896a30.js](#) (script, 34.96 KB)
- GET [verified...scripts.2261e7ce94e7bda05750.js](#) (script, 2.75 KB)
- GET [verified...main.025a0d6e80f02278b503.js](#) (script, 356.45 KB)
- GET [verified...js-ah...nrspa-1169.min.js](#) (script, 36.67 KB)
- GET [tms.cap...Bootstrap.js](#) (script, 85.23 KB)
- GET [bfp.cap...browserFingerPrint1.min.js](#) (script, 0 B)
- GET [verified...uba.js](#) (script, 7.46 KB)
- GET [verified...web_properties.js](#) (script, 1.57 KB)
- GET [device...ccj1tho=sic_0145b1ea-7aa0-4472](#) (script, 31.09 KB)
- GET [tms.cap...serverComponent.php?r=5715628](#) (script, 524 B)
- GET [w.usabil...45796c56d2a3j?r=1](#) (script, 157 B)
- GET [su.coh...6j?r=namespace+cofdrp](#) (script, 1.29 KB)
- GET [tms.cap...99c471592229a8e4bb115da896a0](#) (script, 99.27 KB)
- GET [tms.cap...0eb5b22ec0d871a30010d833c8bd](#) (script, 0 B)
- GET [tms.cap...c06a5cd2ee1ebf4a25a5b30cc97e](#) (script, 31.55 KB)
- GET [bam...c344d59e907a=7956961918aa=1d](#) (script, 275 B)

The developer tool also shows response headers for the selected request, including "Cache-Control: no-cache, no-store, must-revalidate", "Connection: keep-alive", "Content-Encoding: gzip", "Content-Type: application/javascript; charset=UTF-8", "Date: Wed, 06 Jan 2021 16:10:24 GMT", "Expires: Wed, 06 Jan 2021 16:10:24 GMT", "Pragma: no-cache", "Transfer-Encoding: chunked", and "Vary: Accept-Encoding, X-Ion-Msg, prod".

Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

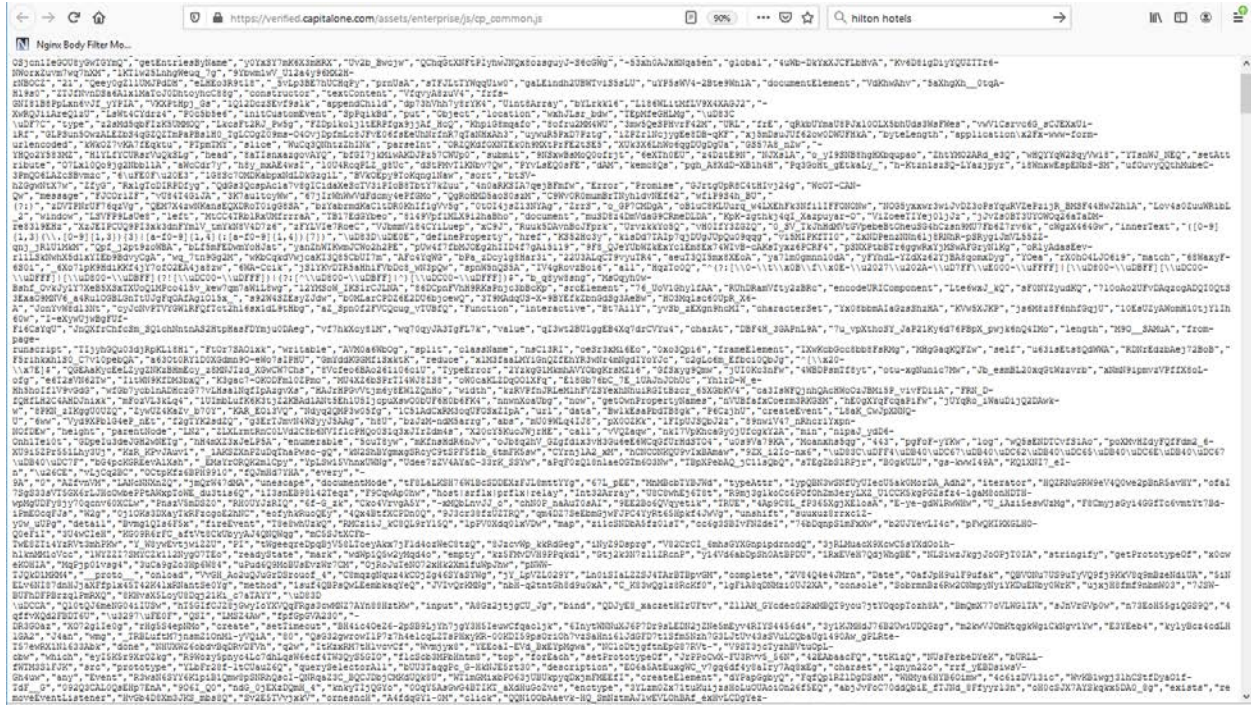
360. The Accused Capital One Products and Services select, via the processor, presentation information corresponding to the transactional information to transmit from the server to the client device, the presentation information specifying how the transactional information is to be displayed. For example, the Capital One server receives presentational information corresponding to the transactional information. The presentation information is used to display and interact with the transactional information on the web page of the Capital One customer device or client device. *Id.*

361. The Accused Capital One Products and Services transmit, via the processor, at least one message including the presentation and transactional information from the server to the client device. A message from the Capital One server is sent containing presentation and transactional information, the message is further sent to at least the F5 server. The message received by the

Capital One customer device or client device further includes at least the presentation information and transactional information.

362. The Accused Capital One Products and Services determine 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. For example, information is sent to at least the F5 server from the Capital One servers based on the Capital One customer device or client device. The F5 server modifies the presentation information to obscure the existence of the transactional information from malicious code. The modified code is sent back to the Capital One server. A review of source website code for the corporate website of Capital One demonstrate that the website obfuscates the source code constantly, to prevent automated attacks. The Java Script code shows that Capital One changes the source code constantly, to prevent automated attacks. An acceptable response must be via the server to recover the inverse transform or additional code. Moreover, Capital One's website includes source code stored on Capital One servers that discerns the type of display utilized by the Capital One customer device or client device, which is communicated to the Capital One web server and the F5 web server as part of the request by the Capital One customer device or client device to visit the Capital One webpage. The HTML presentation information code stored on the Capital One webserver must be anchored to the Capital One customer device or client device display device and pixel locations become important. This code developed by Capital One and shared with F5 as part of the Accused Capital One Products and Services is integral in the Capital One implementation. The transactional information such as user ID / username and password of the Capital One customer

device or client device, and as programmed on the Capital One webpage, must match the registered security information for the client.



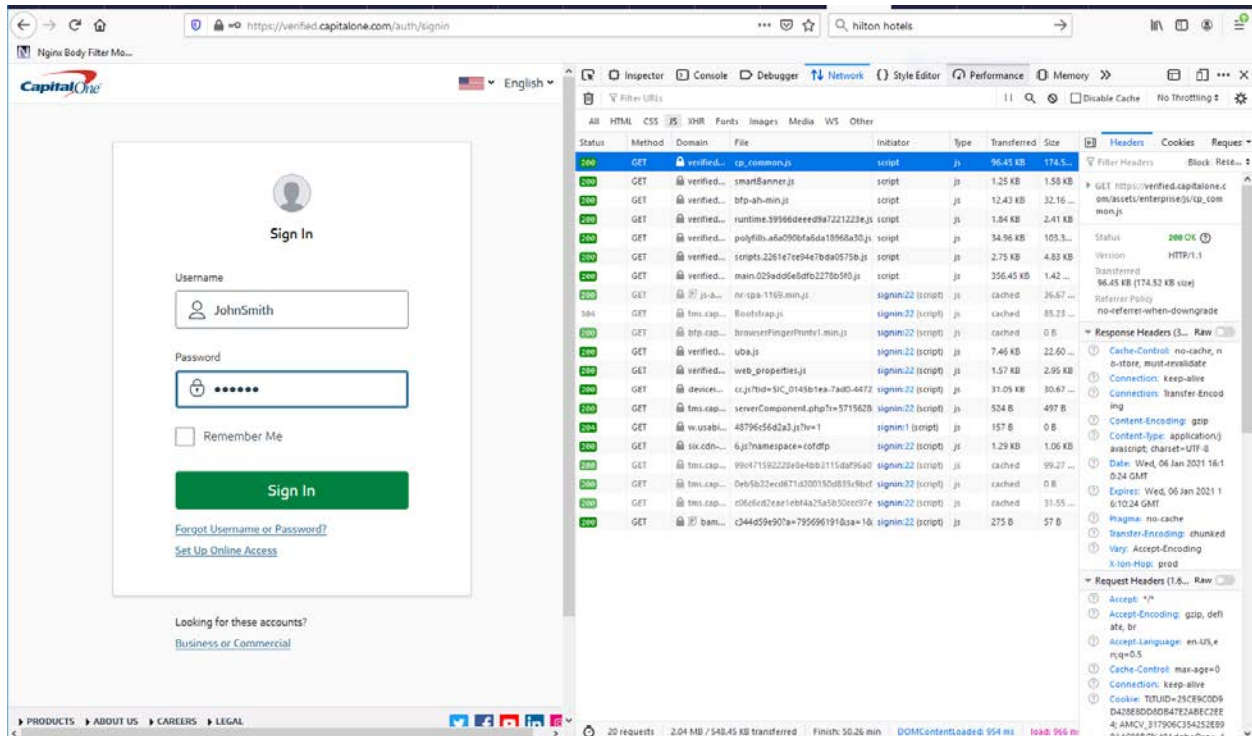
Capital One Customer Sign In Webpage, available at <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

363. The Accused Capital One Products and Services, receive, in the processor, the response message from the client device. For example, the Capital One servers receive the response message from the Capital One customer device or client device.

364. The Accused Capital One Products and Services, responsive to information in the response message not matching the prediction, provide, via the processor, an indication that 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. For example, the Capital One webpage includes alterations in the website source code. In the Accused

Capital One Products and Services, the acceptable response is further determined by estimating locations of rendered features and functions as displayed by the client device, estimating locations of rendered page geometry of the features and functions, and estimating relative locations between text, input boxes, buttons, and advertisements as displayed by the client device. *Id.*

365. In the Accused Capital One Products and Services 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. The presentation information includes at least soft information in the form of code, usually HTML/CSS/JavaScript for rendering, displaying, and interacting with a web page that often displays hard (transactional) information. The presentation information is designed and developed by or on behalf of Capital One.



Capital One Customer Sign In Webpage, *available at* <https://verified.capitalone.com/auth/signin> (last visited Jan. 15, 2021).

366. In the Accused Capital One Products and Services 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. For example, transactional information includes at least the coding and variables surrounding the hard information, such as a user ID / username or password, that is essential to completing the transaction such as a login. The transactional information is designed and develop by or on behalf of Capital One. *Id.*

367. The Accused Capital One Products and Services satisfy each and every element of each asserted claim of the '537 Application either literally or under the doctrine of equivalents.

368. Capital One's infringing activities are and have been without authority or license under the '537 Application.

369. SunStone is entitled to recover from Capital One the damages sustained by SunStone as a result of Capital One's infringing acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court, pursuant to 35 U.S.C. § 284.

TWELFTH CAUSE OF ACTION
(Capital One's Indirect Infringement of the '537 Application
[U.S. Patent No. 10, __, __] pursuant to 35 U.S.C. § 271(b))

370. SunStone repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

371. As set forth above, Capital One is liable for indirect infringement under 35 U.S.C. § 271(b) of at least 1-9 and 21-30 of the '537 Application at least as early as service of the Complaint because it knowingly encourages, aids, and directs others (e.g., end users and customers) to use and operate the Accused Capital One Products and Services in an infringing manner and to perform the claimed methods of the '537 Application.

372. Since at least as early as service of this original Complaint, has had knowledge of the '537 Application. Since that time, Capital One has specifically intended, and continues to specifically intend, for persons who acquire and use the Accused Capital One Products and Services, including Capital One's customers, to use the Accused Capital One Products and Services in a manner that infringe the '537 Application. This is evident when Capital One encourages and instructs customers and other end users in the use and operation of the Accused Capital One Products and Services via advertisement, technical material, instructional material, and otherwise.

373. Capital One specifically intends the Accused Capital One Products and Services to be used and operated to infringe one or more claims, including at least Claims 1-9 and 21-30 of the '537 Application.

374. Capital One encourages, directs, aids, and abets the use, configuration, and installation of the Accused Capital One Products and Services.

375. As detailed above, Capital One has instructed its customers to use the accused methods and Accused Capital One Products and Services in an infringing manner.

376. Capital One's analysis and knowledge of the '537 Application combined with its ongoing activity demonstrates Capital One's knowledge and intent that the identified features of its Accused Capital One Products and Services be used to infringe the '537 Application.

377. Capital One's knowledge of the '537 Application and SunStone's infringement allegations against Capital One combined with its knowledge of the Accused Capital One Products and Services and how they are used to infringe the '537 Application, consistent with Capital One's promotions and instructions, demonstrate Capital One's specific intent to induce users of the Accused Capital One Products and Services to infringe the '537 Application.

378. SunStone is entitled to recover from Capital One compensation in the form of monetary damages suffered as a result of Capital One'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

379. SunStone hereby demands a trial by jury of all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

SunStone prays for the following relief:

(A) An entry of judgment that F5 has infringed and is directly infringed the '870 Patent, the '759 Patent, and the '537 Application;

(B) An entry of judgment that F5 has infringed and is indirectly infringed the '870 Patent, the '759 Patent, and the '537 Application;

(C) An entry of judgment that Capital One has infringed and is directly infringed the '870 Patent, the '759 Patent, and the '537 Application;

(D) An entry of judgment that Capital One has infringed and is indirectly infringed the '870 Patent, the '759 Patent, and the '537 Application;

(E) Judgment that the '870 Patent, the '759 Patent, and the '537 Application are valid and enforceable;

(F) A preliminary and permanent injunction against F5 and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the '870 Patent, the '759 Patent, and the '537 Application and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

(G) A preliminary and permanent injunction against Capital One and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing the '870 Patent, the '759 Patent, and the '537 Application and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

(H) An award to SunStone of such damages as it shall prove at trial against F5 that is adequate to fully compensate SunStone for F5's infringement of the '870 Patent, the '759 Patent, and the '537 Application, said damages to be no less than a reasonable royalty;

(I) An award to SunStone of such damages as it shall prove at trial against Capital One that is adequate to fully compensate SunStone for Capital One's infringement of the '870 Patent, the '759 Patent, and the '537 Application, said damages to be no less than a reasonable royalty;

(J) A determination that damages against F5 are available under 35 U.S.C. § 154(d);

(K) A determination that damages against Capital One are available under 35 U.S.C. § 154(d);

(L) A determination that F5's infringement has been willful, wanton, deliberate, and egregious;

(M) A determination that Capital One's infringement has been willful, wanton, deliberate, and egregious;

(N) A determination that the damages against F5 be trebled or for any other basis within the Court's discretion pursuant to 35 U.S.C. § 284;

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

(P) A finding that this case against F5 is "exceptional" and an award to SunStone of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

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

(R) An accounting of all infringing sales and revenues of F5, together with post judgment interest and prejudgment interest from the first date of infringement of the '870 Patent, the '759 Patent, and the '537 Application;

(S) An accounting of all infringing sales and revenues of Capital One, together with post judgment interest and prejudgment interest from the first date of infringement of the '870 Patent, the '759 Patent, and the '537 Application; and

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

Dated: January 22, 2021

Respectfully submitted,

By: /s/ Cecil E. Key
Bernard J. DiMuro, Esq. (VSB No. 18784)
Michael S. Lieberman, Esq. (VSB No. 20035)
Jonathan R. Mook, Esq. (VSB No. 19177)
DIMUROGINSBERG P.C.
1101 King Street, Suite 610
Alexandria, Virginia 22314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
Email: bdimuro@dimuro.com
mlieberman@dimuro.com
jmook@dimuro.com

Cecil E. Key, Esq. (VSB No. 41018)
KEY IP LAW GROUP, PLLC
1934 Old Gallows Road, Suite 350
Vienna, Virginia 22182
Telephone: (703) 752-6276
Facsimile: (703) 752-6201
Email: cecil@keyiplaw.com

Of Counsel:

Christopher E. Hanba
Texas Bar No. 24121391 (*Pro Hac Vice Pending*)
Cabrach J. Connor
Texas Bar No. 24036390 (*Pro Hac Vice Pending*)
CONNOR KUDLAC LEE PLLC
609 Castle Ridge Road, Suite 450
Austin, Texas 78746
Phone: (512) 777-1254
Fax: (888) 387-1134
chris@connorkudlaclee.com
cab@connorkudlaclee.com

Attorneys for Plaintiff
SunStone Information Defense, Inc.