AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court NDCA on the following X Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
CV 13-05808 DMR	12/16/2013	Oakland Division, 1301 Clay St., Suite 400S, Oakland, CA 94612

PLAINTIFF	DEFENDANT
FINJAN INC	PROOFPOINT INC ET AL

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,058,822		
2	7,647,633	SEE ATTACHED	
3	6,154,844		
4	7,975,305		
5	8,225,408		

In the above—entitled case, the following patent(s) have been included:

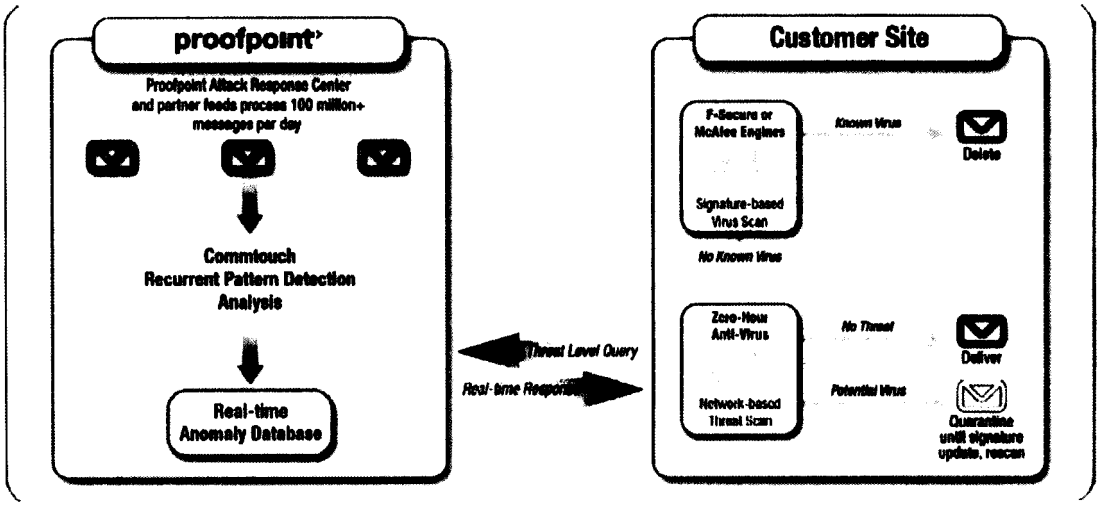
DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,079,086		
2 8,141,154		
3 7,613,918		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Valerie Kyono	December 17, 2013

Copy 3 - Upon termination of action, mail this copy to Commissioner

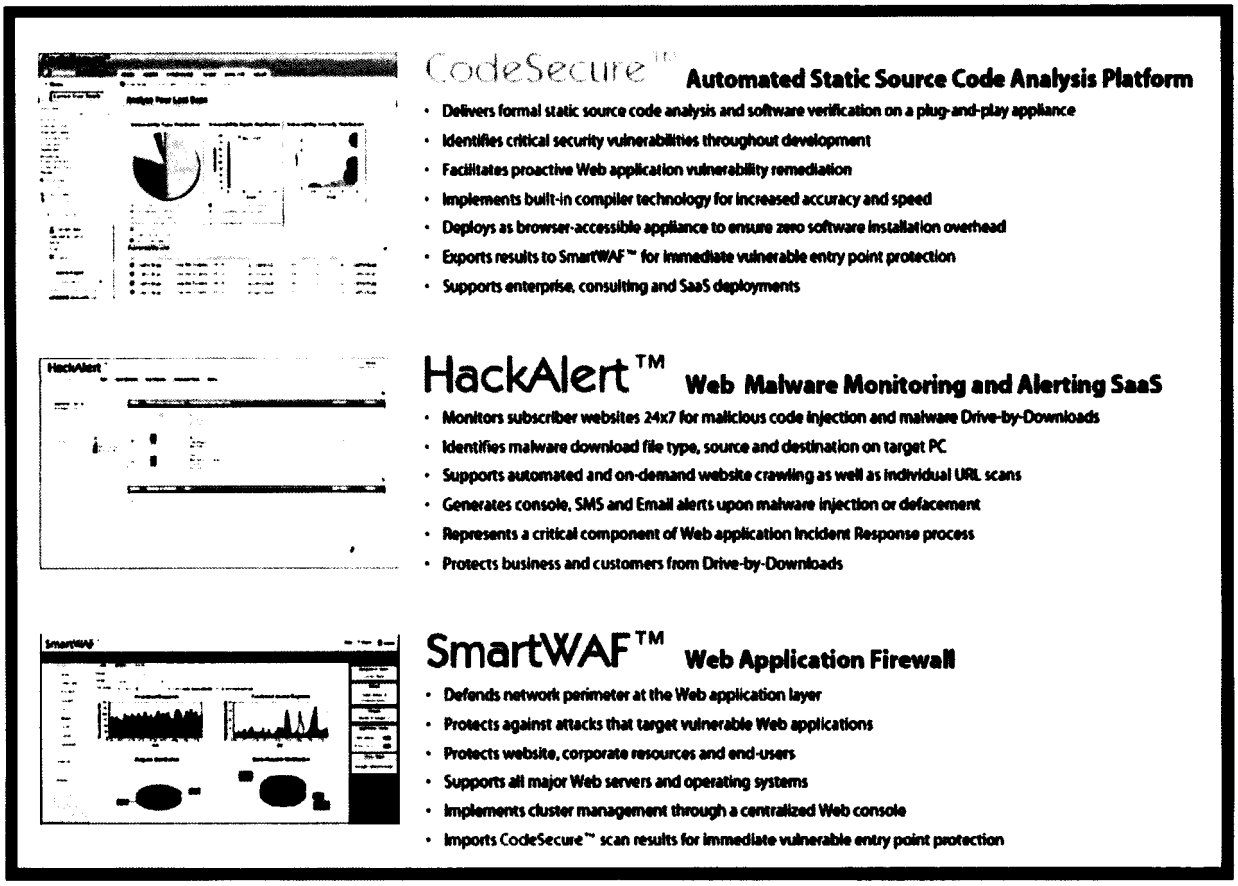


See WP-Proofpoint-Close-the-Zero-Hour-Gap (attached as Exhibit I).

38. Proofpoint's Targeted Attack Protection and Malware Analysis Service (also known as Next Generation Detection) allow unknown malicious attacks that are missed by traditional signature based detection to be caught. Proofpoint's Malware Analysis Service utilizes anomalytics to identify suspicious files and begins the process of analyzing the files in a sandbox for signs of a malware attack. DS-Proofpoint-Targeted-Attack-Protection (attached as Exhibit J).

39. On September 5, 2013, a wholly-owned subsidiary of Proofpoint merged with and into Armorize Technologies, Inc. ("Armorize"), with Armorize surviving as a wholly-owned subsidiary of Proofpoint. Armorize develops and markets SaaS anti-malware products and real-time dynamic detection of next generation threats. Proofpoint Form 10-Q (attached as Exhibit K).

40. Proofpoint paid $25,000,000 in cash for Armorize and has been utilizing Armorize technologies in Proofpoint's products for nearly a year before the acquisition. See Proofpoint, Inc. to Acquire Armorize Technologies, Inc.pdf (attached as Exhibit L). Armorize products include HackAlert Anti-Malware, CodeSecure Automated Static Source Code Analysis and SmartWAF Web Application Firewall. Information concerning these products is shown below:



See Armorize Technologies End-to-End Web Application Security (attached as Exhibit M).

41. Armorize, now integrated into Proofpoint, uses, sells, offers for sale, and/or imports into the United States and this District products and services that utilize HackAlert Anti-Malware, CodeSecure Automated Static Source Code Analysis and SmartWAF Web Application Firewall, including but not limited to the following: HackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert CodeSecure, HackAlert Vulnerability Assessment and SmartWAF.

42. HackAlert is a service that analyzes, detects, prevents, and mitigates malware infections in online advertisements, documents and e-mails. HackAlert focuses on scanning for zero-day malware and exploits used in Advanced Persistent Threat ("APT") attacks, which are undetectable by typical virus or malware scanners. HackAlert's sandbox analyzes these zero-day exploits and APT, such as malicious binaries, document exploits (PDF, Word, Excel, PowerPoint, Flash), Java exploits, browser exploits, drive-by downloads and click-to downloads. *See* Take APT Malware By Storm (attached as Exhibit N).

43. CodeSecure is an automatic static code analysis platform that identifies security vulnerabilities and works with SmartWAF and HackAlert to provide vulnerability entry point protection. CodeSecure identifies vulnerabilities such as Cross Site Scripting, File Inclusion, Malicious File Execution, Information Leakage and SQL Injection. CodeSecure checks for vulnerabilities based on algorithms to determine behavior outcomes of input data. *See* CodeSecure (attached as Exhibit O).

44. SmartWAF is a web application firewall. It defends against web application attacks such as SQL Injection, Cross Site Scripting, Cross Site Request Forgery, Cookie Tampering, Directory Indexing, Information Leakage, Content Spoofing, Application Fingerprinting and Web Server Fingerprinting. SmartWAF may also integrate with CodeSecure by importing source code analysis findings and reconfiguring its rule set to block web application exploits targeted at vulnerabilities identified by CodeSecure.

45. Armorize deploys a developers' API for HackAlert Scanning and Forensics Extraction for Malware. With the API, developers can detect malware not normally caught by normal anti-virus technologies, such as zero-day exploits or Advanced Persistent Threats; automatically induce malware behavior and collect forensics information; and scan individual URLs for Web malware,

such as drive-by downloads and click-to downloads, and generate trackbacks, exploitation steps, JavaScript execution and malware execution. *See* APT-malware-malvertising-scanning-api (attached as Exhibit P).

DEFENDANT'S INFRINGEMENT OF FINJAN'S PATENTS

46. Defendants have been and are now infringing the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent, the '154 Patent and the '918 Patent (collectively "the Patents-In-Suit") in this judicial District, and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale the claimed systems and methods that utilize Proofpoint's Zero-Hour Threat Detection, Proofpoint's Malware Analysis Service, Proofpoint's Targeted Attack Protection, HackAlert, and CodeSecure, including without limitation on Proofpoint Enterprise Protection, Proofpoint's Targeted Attack Protection, Proofpoint Essentials, Proofpoint Protection Server, Proofpoint Messaging Security GatewayHackAlert Suite, HackAlert Website Monitoring, HackAlert Safe Impressions, HackAlert SafeImpressions, HackAlert CodeSecure, HackAlert Vulnerability Assessment and SmartWAF..

47. In addition to directly infringing the Patents-In-Suit pursuant to 35 U.S.C. § 271(a) either literally or under the doctrine of equivalents, Defendants indirectly infringe the '822 Patent, the '633 Patent, the '844 Patent, the '305 Patent, the '408 Patent, the '086 Patent and the '918 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its users and developers, to perform all or some of the steps of method claims of the Patents-In-Suit, either literally or under the doctrine of equivalents.

COUNT I

(Direct Infringement of the '822 Patent pursuant to 35 U.S.C. § 271(a))

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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.