JONATHAN K. LEVINE (SBN: 220289)
ELIZABETH C. PRITZKER (SBN: 146267)
SHIHO YAMAMOTO (SBN: 264741)
PRITZKER LEVINE LLP
180 Grand Avenue, Suite 1390
Oakland, California 94612
Telephone: (415) 692-0772
Facsimile: (415) 366-6110
Email: jkl@pritzkerlevine.com;
ecp@pritzkerlevine.com;
sy@pritzkerlevine.com

JOHN A. KEHOE
PRITZKER LEVINE LLP
41 Madison Avenue, 31st Floor
New York, New York 10010
Telephone: (917) 525-2190
Facsimile: (917) 525-2184
Email: jak@pritzkerlevine.com

Attorneys for Plaintiff Sterling International Consulting Group

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

STERLING INTERNATIONAL CONSULTING GROUP, on behalf of itself and all others similarly situated,

Plaintiff,

v.

LENOVO (UNITED STATES) INC., LENOVO GROUP LIMITED, and SUPERFISH INC.,

Defendants.

Case No:

CLASS ACTION

COMPLAINT FOR:
1) VIOLATION OF COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030, *et seq.*);
2) VIOLATION OF FEDERAL WIRETAP ACT (18 U.S.C. § 2510, *et seq.*);
3) VIOLATION OF THE STORED COMMUNICATIONS ACT (18 U.S.C. § 2701, *et seq.*);
4) VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, PENAL CODE §§ 631, 637.2;
5) VIOLATION OF CALIFORNIA BUS. & PROF. CODE § 17200, *et seq.*;
6) TRESPASS TO CHATTELS;
7) COMMON LAW FRAUD; and
8) NEGLIGENT MISREPRESENTATION

DEMAND FOR JURY TRIAL

Plaintiff Sterling International Consulting Group ("Plaintiff"), by and through its undersigned attorneys, hereby complains against defendants Lenovo (United States) Inc. and Lenovo Group Limited (collectively, "Lenovo") and Superfish Inc. (collectively, "Defendants"), on behalf of itself and all others similarly situated, as follows. Plaintiff's allegations are based upon information and belief, except as to its own actions, which are based on knowledge. Plaintiff's information and belief is based on the investigation of its undersigned counsel, and the facts that are a matter of public record, as follows:

NATURE OF THE CASE

1. Lenovo is a $39 billion global Fortune 500 company and the world's largest seller of Windows-based personal computers, with a 20 percent market share. In the fourth quarter of 2014 (September through December 2014), Lenovo sold 16 million personal computers.

2. In August or September 2014, Lenovo began preinstalling a software program called Superfish Visual Discovery on at least 43 different Windows-based Lenovo notebook computer models sold to consumers. Notably, Lenovo did not preinstall the Superfish program on any of its computer models that were marketed to businesses or more sophisticated computer users. The Superfish program was developed, sold and maintained by defendant Superfish Inc., a non-public software company headquartered in Palo Alto, California.

3. The Superfish program is spyware that allowed Lenovo and Superfish Inc. to access and then inject advertising into otherwise secure HTTPS pages that a consumer using one of the affected Lenovo notebook computers was viewing on the internet. The Superfish program does this by performing what is known as a "man-in-the-middle attack" that essentially hijacks the consumer's viewing session by breaking Windows' encrypted web connections, bypassing the secure root certificates in the computer's root store or root directory, and replacing them with a single common self-signed Superfish root certificate. All of this occurs without the user's knowledge.

4. Lenovo never disclosed that it was preinstalling the Superfish program

on millions of notebook computers it was selling to consumers. Rather, the Superfish program was buried deep within the operating system at a root level that would generally avoid disclosure, operate without the knowledge of the computer user, and not be identified as spyware, malware or adware by any of the common computer security programs sold or provided for free with new personal computers by Microsoft, McAfee or Symantec.

5. Lenovo never disclosed the Superfish program and took affirmative steps to conceal it from consumers because the program is generally considered to be spyware, adware or malware and, aside from the fact that it allows companies to spy on user's every move online, the program also creates serious security issues for any consumer accessing the internet with a Lenovo notebook computer on which the Superfish program has been installed. By using a single self-signed root certificate on all of the affected Lenovo notebook computers, the Superfish program intentionally creates a large hole in each computer's browser security that would easily allow Lenovo and Superfish or anyone on the same wireless network (such as an airport or café) to hijack that browser and silently collect any bank credentials, confidential communications, passwords and any other information of value that might be there.

6. Additionally, the large security hole created by the Superfish program can easily be breached, because the security key for the single self-signed root certificate used by the Superfish program has been broken and published on the internet. It took one computer security researcher less than 15 seconds on-line to obtain the security key for the Superfish root certificate. The Electronic Frontier Foundation and other computer security companies have reported that the security problems associated with the Superfish program infect not only consumers using the Internet Explorer web browser on their Lenovo notebook computers, but also Google Chrome, Firefox, Opera and Safari for Windows.

7. Lenovo now admits that the Superfish program creates a "high" security risk for any notebook computer on which it was preinstalled and the U.S. Department of

Homeland Security has taken the extraordinary step of issuing an alert advising consumers with an affected Lenovo notebook computer to remove the program immediately because it makes the computer vulnerable to cyberattacks, even if it is running anti-virus and firewall protection programs. As one computer expert noted last week after the full story was revealed, it's "quite possibly the single worst thing I have seen a manufacturer do to its customer base . . . I cannot overstate how evil this is." Another commentator stated that "[w]hen Lenovo preinstalled Superfish adware on its laptops, it betrayed its customers and sold out their security."

8. Lenovo has since acknowledged that because of consumer complaints, in January 2015 it stopped preinstalling the Superfish program on newly manufactured notebook computers and shut down the server connections with Superfish Inc that enabled the program to operate. But Lenovo did not disclosed this information to the consumers who already had purchased any of the affected Lenovo notebook computers and is reported to have continued to ship already manufactured Lenovo notebook computers through early February with the program still installed.

9. In fact, when Lenovo did speak about the program on its user forums, it continued to claim that it was beneficial to consumers and did not warn them of the high security risk. For example, on January 23, 2015, a Lenovo administrator responded on a Lenovo users forum to consumer complaints about the program as follows: "Superfish comes with Lenovo consumer products only and is a technology that helps users find and discovery products visually. The technology instantly analyzes images on the web and presents identical and similar product offers that may have lower prices, helping users search for images without knowing exactly what an item is called or how to describe it in a typical text-based search engine."

10. The truth finally came out on February 20, 2015, when a Google programmer purchased a Lenovo notebook computer with the Superfish program installed and then wrote about his experience, which quickly went viral. Lenovo at first downplayed the scope of the problem. It claimed that the Superfish program was only

installed on some consumer notebook computers shipped in a short window between October and December 2014. But, it has subsequently admitted that the Superfish program actually was installed on at least 43 different notebook computer models shipped from September 2014 through February 2015, including some of Lenovo's most popular notebook computer models.

11. Lenovo now claims that the Superfish program has only recently been disabled and poses no threat to consumers who have it installed on their Lenovo notebook computers. But, even if the Superfish program is disabled, or even uninstalled, this does not by itself remove the self-signed root certificate that creates the high security issues that are so problematic. And Lenovo executives continue to assert that the security issues that have been raised are only "theoretical concerns."

12. Even though many computer security experts are recommending that any Lenovo notebook computer that has the Superfish program preinstalled be completely wiped clean and that a new Windows operating system be installed, all that Lenovo has done to date is to post on its website lengthy instructions on how a consumer can uninstall the program and the root certificate, and a program that will do that for the consumer.

13. And, while Lenovo's Chief Technology Officer, Peter Hortensius, has now admitted that "we messed up badly" and that "we just flat-out missed it on this one, and did not appreciate the problem it was going to create," Lenovo has not: (a) attempted to affirmatively notify all consumers who own the affected notebook computers that their computers are not secure; (b) offered to provide any reimbursement or compensation for any damages the Superfish program may have caused; (c) offered to provide technical assistance to consumers who may not have the skill to remove the Superfish program and certificate from their computer; (d) offered any type of credit monitoring to consumers whose personal information may have been compromised; (e) offered to assist consumers who may want their computer wiped clean and have a new operating system installed; or (f) offered any refunds to any consumers who no longer feel safe using their Lenovo

notebook computers.

14. Superfish Inc., for its part, continues to claim that the Superfish program does not present any security risks, and that any problems with the single self-signed root certificate used by its program are the fault of a third-party developer that created the certificate for Superfish.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this matter pursuant to 18 U.S.C. § 1030(g) and 28 U.S.C. §§ 1331.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law occurred in this District, defendant Superfish Inc. is headquartered in this District, and Lenovo conducts business with and sold affected Lenovo notebook computers directly to consumers in this District.

PARTIES

17. Plaintiff Sterling International Consulting Group purchased a new Lenovo notebook computer on which the Superfish program was preinstalled. Plaintiff is a Delaware corporation with its principal place of business in Statesville, North Carolina.

18. Defendant Lenovo (United States) Inc. is a Delaware corporation with its principal place of business located in Morrisville, North Carolina. Lenovo (United States) Inc. is a wholly-owned subsidiary of defendant Lenovo Group Limited.

19. Defendant Lenovo Group Limited is a Hong Kong corporation with its principal place of business located in Beijing, China. Lenovo Group Limited is the parent of defendant Lenovo (United States) Inc.

20. Defendant Superfish Inc. is a Delaware corporation with its principal place of business in Palo Alto, California.

//

//

//

FACTUAL ALLEGATIONS

21. Lenovo was founded in Beijing, China in 1984 and grew to become China's leading personal computer company. Lenovo's business went global in 2005 when it acquired IBM Corporation's personal computer business. As a result of that acquisition, Lenovo became the world's third largest personal computer company. Since then, it has risen to become the world's largest personal computer company.

22. Lenovo publicly touts the "Lenovo Way," which it claims means "We Do What We Say. We Own What We Do." Lenovo claims that it "builds the world's leading technology" into all of its products and that it is "committed to ensuring that our products are safe." Lenovo also represents that it's "products comply with the laws and regulations into each country we ship. Lenovo products are designed, tested and approved to meet worldwide standards for Product Safety, Electromagnetic Compatibility, Ergonomics and other regulatory compulsory requirements, when used for their intended purpose."

23. Superfish Inc. was founded in 2006 by its CEO, Adi Pinhas, who has a long history working in industrial and military surveillance in the United States and Israel. The company, based in Palo Alto, California, is not public and has been financed to date by five venture capital firms, including two firms based in Palo Alto and three based in Israel. It had $38 million in revenue in 2014. Superfish calls itself a visual search company.

24. According to David Auerbach, a technology writer and software engineer, Superfish "has a long history of disseminating adware, spyware, malware, and crapware." Computer security researcher Robert Graham, who was able to obtain and break the security of the Superfish root certificate in only a few minutes, is even more critical of the company:

> The company claims it's providing a useful service, helping users do price comparisons. This is false. It's really adware. They don't even offer the software for download from their own website. It's hard Googling for the software if you want a copy because your search results will be filled with

> help on removing it. The majority of companies that track adware label this as adware.
>
> Their business comes from earning money from those ads, and it pays companies (like Lenovo) to bundle the software against a user's will. They rely upon the fact that unsophisticated users don't know how to get rid of it, and will therefore endure the ads.

25. In approximately August or September 2014 or earlier, Lenovo began preinstalling the Superfish Visual Discovery software program on at least 43 different Windows-based Lenovo notebook computer models. All 43 models (listed below) were marketed and sold primarily to consumers. Lenovo did not preinstall the Superfish program on any of its computer models that were marketed and sold primarily to businesses or more sophisticated computer users.

26. The Lenovo notebook computer models on which the Superfish program was installed include the following:

G Series:	G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45
U Series:	U330P, U430P, U330Touch, U430Touch, U530Touch
Y Series:	Y430P, Y40-70, Y50-70
Z Series:	Z40-75, Z50-75, Z40-70, Z50-70
S Series:	S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch
Flex Series:	Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10
MIIX Series:	MIIX2-8, MIIX2-10, MIIX2-11
YOGA Series:	YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW
E Series:	E10-20

27. The purpose of the Superfish Visual Discovery program was to allow

Lenovo and Superfish to access and then inject advertising into otherwise secure HTTPS pages on the internet that a consumer using one of the affected Lenovo notebook computers was viewing. Put more simply, without any disclosure to the user, the Superfish program altered the user's internet search results to display different ads than the user would otherwise see. According to the New York Times, the program "could track customers' every online move, intercept secure web sessions and render their computers vulnerable to hackers."

28. Any web browser that uses HTTPS correctly needs a way to verify the certificates that link sites' domain names to the cryptographic public keys they use. This is accomplished by having a list of the root certificate authorities maintained in the operating system in a root store or root directory that can sign certificates that the browser will trust. The Superfish program breaks this secure encryption method by bypassing the legitimate and secure root certificates and replacing them with Superfish's version. This is known as a "man-in-the-middle attack" and it is not visible to the computer user.

29. Neither Lenovo nor Superfish ever disclosed that Lenovo was preinstalling the Superfish program on millions of notebook computers it was selling to consumers. In fact, the Superfish program was buried deep within the operating system at a level that would generally avoid disclosure, operate without the knowledge of the computer user, and not be identified as spyware, malware or adware by any of the common computer security programs sold or provided for free with new personal computers. As CNET magazine noted in a recent critical article about Lenovo and the Superfish program, "[a]nother reason why Superfish is unusually dangerous is that it's not an app like Adobe Photoshop or Microsoft Word, but rather code hidden from everyday users."

30. As the New York Times reported: "The company [Lenovo] buried its software in the lowest level of a PC's operating system, precisely where customers and antivirus products would never detect it, and had been siphoning data back to servers belonging to Superfish, an Israeli software company with headquarters in Silicon Valley

that markets itself as a visual search company."

31. Lenovo never disclosed the Superfish program and took affirmative steps to hide it from consumers because the program is generally considered to be spyware, adware or malware and it creates serious security issues for any consumer accessing the internet with a Lenovo notebook computer on which the Superfish program has been installed. It is no coincidence that Lenovo only preinstalled the program on computer models being marketed and sold to consumers and not on its models that were directly marketed and sold to business and professionals.

32. By using a single self-signed root certificate on all of the affected Lenovo notebook computers, the Superfish program intentionally creates a hole in each computer's browser security that would easily allow Lenovo and Superfish, or anyone on the same wireless network, to hijack that browser and, without the knowledge of the user, collect whatever information is being transmitted, including personal financial information such as credit card numbers or bank credentials, passwords, or any confidential personal or business information.

33. The security hole created by the Superfish program can easily be breached because the security key for the Superfish root certificate has been repeatedly broken and is now widely available on the internet. Computer security companies have reported that the security problems associated with the Superfish program potentially impact consumers using all of the major web browsers, including Internet Explorer, Google Chrome, Firefox, Opera and Safari for Windows.

34. Lenovo now acknowledges that the Superfish program creates a "high" security risk for any notebook computer on which it was preinstalled. And the U.S. Department of Homeland Security has issued an alert advising consumers with an affected Lenovo notebook computer to remove the program immediately because it makes the computer vulnerable to cyberattacks, even if it is running anti-virus and firewall protection programs.

35. Noted computer security researcher Marc Rogers wrote that it's "quite

possibly the single worst thing I have seen a manufacturer do to its customer base . . . I cannot overstate how evil this is." Another commentator stated that "[w]hen Lenovo preinstalled Superfish adware on its laptops, it betrayed its customers and sold out their security." And the Electronic Frontier Foundation, writing about the actions of Lenovo and Superfish, stated that "[u]sing a MITM [man-in-the-middle] certificate to inject ads was an amateurish design choice by Superfish. Lenovo's decision to ship this software was catastrophically irresponsible and an utter abuse of the trust their customers placed in them." The New York Times is equally critical of Lenovo and Superfish: "What makes the latest discovery so disconcerting is that if a government or company can plant spyware in the lowest level of a machine, it can steal your passwords, serve up any web page, steal your encryption keys and control your entire digital experience, undetected."

36. Lenovo has since acknowledged that at some point in January 2015, customer complaints caused it to stop preinstalling the Superfish program on newly manufactured notebook computers and to shut down the server connections with Superfish that enabled the program to operate. However, Lenovo made no effort to inform consumers who already had purchased any of the affected Lenovo notebook computers and the company is reported to have continued to ship already manufactured notebook computers through early February with the program still installed, even if it was no longer operational.

37. In fact, at the same time that Lenovo internally had decided to shut down the program because of customer complaints, it publicly still was claiming that the Superfish program was beneficial to consumers. For example, on January 23, 2015, a Lenovo administrator responded on a Lenovo users forum to consumer complaints about the program as follows: "Superfish comes with Lenovo consumer products only and is a technology that helps users find and discover products visually. The technology instantly analyzes images on the web and presents identical and similar product offers that may have lower prices, helping users search for images without knowing exactly what an item is called or how to describe it in a typical text-based search engine."

38. On February 20, 2015, Lenovo's surreptitious installation and use of the Superfish program became national news after a Google programmer purchased a Lenovo notebook computer with the Superfish program installed and then went public with his experience. At first, Lenovo downplayed the scope of the problem, claiming that the Superfish program was installed only on some consumer notebook computers shipped in a short window between October and December 2014. But when Lenovo was confronted with customer complaints going back as far as September 2014, it subsequently admitted that the Superfish program actually was installed on at least 43 different notebook computer models shipped at least from September 2014 through February 2015. The 43 models including some of Lenovo's most popular notebook computers.

39. Lenovo has now taken the position that the security issues caused by the Superfish program are only "theoretical concerns" and that, because the program has been disabled, it poses no threat to consumers who have it installed on their Lenovo notebook computers. But, even if the Superfish program is disabled, or even uninstalled, this does not by itself remove the self-signed root certificate that creates the high security issues that are so problematic.

40. Many computer security experts who have looked at the Superfish program and its security issues are recommending that any Lenovo notebook computer that has the program preinstalled be completely wiped clean and that a new Windows operating system be installed. But, all that Lenovo has done to date is to post on its website lengthy instructions on how a consumer can uninstall the program and the root certificate, and a program that will do that for the consumer. Superfish has done nothing other than to continue to claim that its software is somehow beneficial to consumers and to blame a third party developer it hired for any security issues arising from the root certificate used by the Superfish program.

41. Faced with mounting industry reports and criticism on how the Superfish program compromises basic computer security, Peter Hortensius, Lenovo's Chief

Technology Officer, only recently has publicly acknowledged that "we messed up badly" and that "we just flat-out missed it on this one, and did not appreciate the problem it was going to create."

42. While Lenovo now admits that the Superfish program creates a severe security risk for its customers who purchased notebook computers with the program preinstalled, Lenovo has not attempted to directly notify those customers to inform them that their computers are not secure, has not offered to provide any reimbursement or compensation for any damages the Superfish program may have caused, has not offered to provide technical assistance to consumers who may not have the skill to remove the Superfish program and certificate from their computer, has not offered any type of credit monitoring or other protection to consumers whose personal or financial information may have been compromised, has not offered to assist consumers who may want their computer hard drive erased and a new operating system installed, has not pulled affected computers from store shelves, and has not offered any refunds to any consumers who no longer feel safe using their Lenovo notebook computers.

CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of itself and the following Class:

> All natural persons or entities in the United States who purchased or otherwise acquired a Lenovo notebook computer on which the Superfish Visual Discovery software program was preinstalled.

Excluded from the Class set forth above are defendants and their employees, officers and directors, and the judge assigned to this action.

44. The Class is so numerous that joinder of all members is impracticable. While the exact number of Class members is unknown to plaintiff at this time prior to discovery, plaintiff believes that there hundreds of thousands of Class members.

45. Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and other Class members sustained damages and injury arising out of

defendants' common course of conduct in violation of law as complained herein. The injuries and damages of each member of the Class were directly caused by defendants' wrongful conduct as alleged herein.

46. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in complex class action litigation.

47. Common questions of law and fact exist as to all members of the Class, and these common questions predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are whether:

a. Defendants failed to disclose, inadequately disclosed, and/or concealed the pre-installation of the Superfish Visual Discovery program on certain Lenovo notebook computers;

b. Defendants had a duty to disclose (a) above;

c. Defendants violated the Computer Fraud and Abuse Act, as alleged;

d. Defendants violated the Federal Wiretap Act, as alleged;

e. Defendants violated the Stored Communications Act, as alleged;

f. Defendants violated the California Invasion of Privacy Act, as alleged;

g. Defendants engaged in unfair competition violating Section 17200 of the California Business and Professions Code, as alleged;

h. Defendants violated the common law for trespass to chattels, as alleged;

i. Defendants committed the common law tort of fraud, as alleged;

j. Defendants committed the common law tort of negligent misrepresentation, as alleged; and

k. Plaintiff and other members of the Class are entitled to statutory and compensatory damages, restitution, declaratory and injunctive relief, reasonable attorneys' fees and costs.

48. Defendants have acted in a manner applicable to the Class, thereby making final injunctive relief appropriate for the Class as a whole.

49. Plaintiff's claims are typical of those of members of the Class because plaintiff purchased a Lenovo notebook computer on which the Superfish Visual Discovery program was preinstalled.

50. Plaintiff is an adequate representative of the Class and will protect the claims and interests of the Class. Plaintiff does not have interests that conflict with those of the Class. Plaintiff will vigorously prosecute the claims alleged herein and has retained competent counsel with complex class action litigation experience.

51. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all class members is impracticable. The prosecution of separate actions by individual members of the Class would impose heavy burdens upon the courts and defendants, and would create a risk of inconsistent or varying adjudications of the questions of law and fact common to the Class. A class action, on the other hand, would achieve substantial economies of time, effort and expense, and would assure uniformity of decision as to persons similarly situated without sacrificing procedural fairness or bringing about other undesirable results.

52. The interest of members of the Class in individually controlling the prosecution of separate actions is theoretical rather than practical. The Class has a high

degree of cohesion, and prosecution of the action through representatives would be unobjectionable. The amount at stake for each Class member is not great enough individually to enable Class members to maintain separate suits against defendants. Plaintiff does not anticipate any difficulty in the management of this action as a class action.

. **COUNT ONE**

Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq*.

53. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

54. This claim is brought under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* (the "Act"). By virtue of defendants' conduct set forth above, defendants violated Section 1030(a)(5) of the Act, which specifically applies to anyone who:

a. Knowingly causes the transmission of a software program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

b. Intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

c. Intentionally accesses a protected computer without authorization, and a result of such conduct, cases damage.

55. Defendants knowingly caused the installation and operation of the Superfish Visual Discovery program on millions of Lenovo notebook computers sold to consumers in the United States. During both the installation and operation of the Superfish Visual Discovery program, defendants intentionally accessed Class members' computers without authorization and thereby caused damage within the meaning of the Act.

56. During the installation process and operation of the Superfish Visual Discovery program, defendants accessed, installed, and reconfigured essential operating

components of users' operating systems. Defendants' installation and use of malicious software code on plaintiff's and Class members' Lenovo notebook computers was unauthorized.

57. Defendants are liable under the Act, because their actions *either*: (1) intentionally caused damage, (Section 1030(a)(5)(i)); (2) recklessly caused damage (Section 1030(a)(5)(ii)); or (3) simply caused damage (Section 1030(a)(5)(iii)). Under the Act, "damage" is defined to include "any impairment to the integrity of availability of data, a program, a system, or information," that causes "loss to 1 or more persons during any 1-year period . . . aggregating at least $5000 in value . . . ." 18 U.S.C. §§ 1030(e)(8), 1030(a)(5)(B)(i).

58. As described above, defendants failed to disclose that the Superfish Visual Discovery program makes sweeping, dangerous changes to the operating system. As a result of these changes, plaintiff and Class members will have to spend time and labor repairing their Lenovo notebook computers. Additionally, the Superfish Visual Discovery program has consumed the resources and hindered the performance of plaintiff's and Class members' Lenovo notebook computers. Plaintiff and Class members have also lost personal and business opportunities, data and information and goodwill. The harm caused by the installation and operation of the Superfish Visual Discovery program on millions of Lenovo notebook computers will produce aggregate damages far exceeding $5,000.

59. Plaintiff's and Class members' computers are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2)(B). By accessing the internet, these computers are used in interstate commerce and communication.

60. As a direct result of the installation of the Superfish Visual Discovery program and intentional access by defendants to plaintiff's and Class members' computers, defendants caused damage to plaintiff's and Class members' computers.

61. Plaintiff and Class members suffered damages as defined in 18 U.S.C. § 1030(e). As a direct result of defendants' conduct, plaintiff's and Class members'

computers have suffered an impairment to the integrity or availability of data software programs including the operating system. Such impairment has caused and will cause losses aggregating to at least $5,000 in value in any one-year period to plaintiff and Class members.

62. Because of defendants' violation of the Computer Fraud and Abuse Act and pursuant to 18 U.S.C. § 1030(g), plaintiff seeks recovery of compensatory damages and injunctive relief on behalf of itself and Class members.

COUNT TWO

Violation of the Federal Wiretap Act, Title 1 of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*

63. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

64. The Federal Wiretap Act provides a private right of action against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. §§ 2511 and 2520.

65. Defendants intentionally and without the consent of plaintiff and Class members intercepted communications with internet sites and search engines for tortious purposes.

66. Defendants also disclosed to others the content of electronic communications knowing that those communications were unlawfully obtained.

67. Defendants collected plaintiff's and Class members' personal information without consent or compensation.

68. Because of defendants' violation of the Federal Wiretap Act and pursuant to 18 U.S.C. § 2520(a), plaintiff seeks recovery of statutory damages, costs and reasonable attorneys' fees on behalf of himself and Class members.

COUNT THREE

Violation of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*.

69. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

70. The Federal Stored Communications Act provides a private right of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication is provided…." 18 U.S.C. § 2701(a).

71. Defendants intentionally and without the consent of plaintiff and Class members accessed plaintiff's and Class members' Lenovo notebook computers with the intent to find, copy and transmit information on plaintiff's and Class members' computers to servers belonging to Superfish.

72. During the installation and operation of the Superfish Visual Discovery program as herein alleged, defendants intentionally and without plaintiff's and Class members' consent, accessed, found, copied and transmitted plaintiff's and Class Member's "electronic communications," including Internet browsing habits, email communications or other personal information to servers belonging to Superfish, in violation of 18 U.S.C. §§ 2701(a), 2711(1).

73. Plaintiff and Class members have been aggrieved by the intentional and unlawful acts of defendants. As a direct result of the installation and operation of the Superfish Visual Discovery program and intentional access by defendants to plaintiff's and Class members' computers as hereinabove alleged, defendants caused damage to plaintiff and Class members including, but not limited to, the expenses associated with investigating defendants' violations, cleansing or wiping plaintiff's and Class member's computer hard-drives and installing new operating systems, and the prevention of similar violations in the future.

74. Because of defendants' violations of the Stored Communications Act and pursuant to 18 U.S.C. § 2707(b)-(c), plaintiff seeks statutory damages, costs and reasonable attorneys' fees on behalf of itself and Class members.

COUNT FOUR

Violation of the California Invasion of Privacy Act, Penal Code §§ 631 and 637.2

75. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

76. The California Invasion of Privacy Act makes it unlawful, by means of any machine, instrument or contrivance, to purposefully intercept the content of a communication over any "telegraph or telephone wire, line, cable or instrument," or to read, or attempt to read or learn the content of any such communications without the consent of all parties to the communication. California Penal Code § 631(a).

77. Plaintiff's and Class members' internet searches and communications with websites and third parties are communications with the meaning of the Act.

78. Defendants knowingly and willfully intercepted those communications while they were "in transit" using the Superfish Visual Display program and servers that qualify as machines, instruments or contrivances as defined by the Act.

79. Plaintiff and Class members did not consent to and were unaware of defendants' interception of their internet searches and communications, and were injured thereby.

80. Defendants are persons within the meaning of the Act and were not parties to those communications.

81. Defendants' conduct in violation of the Act occurred in California because those acts resulted from business decisions, practices and operating policies that defendants developed, implemented and utilized in California which are unlawful and constitute criminal conduct in defendant Superfish's state of residence and principal place of business and where defendant Lenovo regularly conducts business.

82. As a result of defendants' violations of Section 631 of the California Penal Code, plaintiff and Class members are entitled to relief under Section 637.2 of the California Penal Code, including statutory damages, appropriate declaratory relief and reasonable attorneys' fees.

COUNT FIVE

Violation of the California Bus. & Prof. Code § 17200, *et seq*.

83. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

84. California's Unfair Competition Law (the "UCL") is embodied in California Business and Professions Code § 17200, *et seq*. The UCL defines unfair competition to include any unlawful, unfair or fraudulent business acts or practices. Unlawful acts and practices are those which are in violation of federal, state, county or municipal statutes and regulations.

85. Defendants' conduct as alleged herein constitutes unlawful, unfair and fraudulent business acts and practices, and as a proximate result of those business acts and practices, plaintiff and Class members have suffered harm and lost money and/or property.

86. By engaging in the business acts and practices described herein, defendants have committed one or more acts of unfair competition within the meaning of the UCL.

87. Defendants' business acts and practices are "fraudulent" within the meaning of the Act because they are likely to and did deceive plaintiff and Class members into purchasing and using Lenovo notebook computers preinstalled with the Superfish Visual Display program, resulting in damages and loss to plaintiff and Class members.

88. Defendants' business acts and practices are "unfair" and "unlawful" within the meaning of the Act because those business acts and practices violate the Computer Fraud and Abuse Act, the Federal Wiretap Act, the Stored Communications Act, and the California Invasion of Privacy Act. Plaintiff and Class members were damaged and lost money and/or property as a result.

89. By virtue of the foregoing, and under Cal. Bus. & Prof. Code § 17203, plaintiff and Class members seek injunctive relief and restitution from defendants.

COUNT SIX

Trespass to Chattels

90. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

91. The common law prohibits the intentional intermeddling with a chattel or impairment of the condition, quality or usefulness of the chattel.

92. By engaging in the acts described above without the authorization of plaintiff and Class members. Defendants dispossessed plaintiff and Class members from use and/or access to their computers, or parts of them. Further, these acts impaired the use, value and quality of plaintiff's and Class members' computers. Defendants' acts constituted an intentional interference with the use and enjoyment of the computers that were subject to the Superfish Visual Discovery program. By the acts described above, defendants have repeatedly and persistently engaged in trespass to chattels in violation of the common law.

93. Plaintiff and Class members are entitled to damages in an amount to be determined at trial.

COUNT SEVEN

Common Law Fraud

94. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

95. Defendants have knowingly and/or recklessly engaged in the deceptive practices, uniform misrepresentations and material omissions complained of herein in order to induce plaintiffs and Class members to purchase and use Lenovo notebook computers preinstalled with the Superfish Visual Discovery program that damaged software on those computers and the computers themselves without their knowledge.

96. Plaintiff and Class members had no knowledge of the falsity and/or incompleteness of defendants' misrepresentations when they bought and used their Lenovo notebook computers installed with the Superfish Visual Discovery program.

Plaintiff and Class members relied on defendants' deceptive practices, uniform misrepresentations and omissions to their detriment.

97. Plaintiff and Class members have been damaged as a result of the conduct complained of herein, and the harm or risk of harm is ongoing.

98. Defendants are liable for actual damages to plaintiff and Class members, and their ongoing fraudulent and deceptive conduct should be enjoined.

99. Defendants' conduct in perpetuating the fraud and deceptive practices described above was malicious, willful, wanton and oppressive, or in reckless disregard of the rights of plaintiff and Class members, thereby warranting the imposition of punitive damages against defendants.

COUNT EIGHT

Negligent Misrepresentation

100. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein. Plaintiff brings this claim for relief against all defendants.

101. Defendants had a duty to customers who purchased and used Lenovo notebook computers with the Superfish Visual Display program preinstalled to exercise reasonable care in the design, installation, testing, marketing and sale of those computers.

102. By virtue of the foregoing, defendants breached that duty. As a direct and proximate result of defendants' breach of duty, the Lenovo notebook computers with the Superfish Visual Display program preinstalled performed defectively, as described above.

103. Plaintiff and Class members had no knowledge of the falsity and/or incompleteness of defendants' misrepresentations and/or defects in the Superfish Visual Display program when they purchased and used their Lenovo notebook computers with the Superfish Visual Display program preinstalled. Plaintiff and Class members relied on defendants' deceptive practices, uniform misrepresentations and omissions to their detriment.

104. Plaintiff and Class members have been damaged as a result of the conduct

complained of herein.

105. Defendants are liable for actual damages to plaintiff and Class members.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and the members of the Class request judgment against defendants as follows:

A. An order certifying the Class, directing that this case proceed as a class action, and appoint plaintiff and its counsel to represented plaintiff and the Class;

B. Judgment in favor of plaintiff and Class members in an amount of actual damages, statutory damages or restitution to be determined at trial;

C. An order enjoining defendants from the further activation or use of the Superfish Visual Discovery program in any Lenovo notebook computers:

D. An order granting reasonable attorneys' fees and costs, as well as pre-and post-judgment interest at the maximum legal rate; and

E. Such other and further relief as this Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff on behalf of itself and all others similarly situated hereby requests a jury trial on any and all claims so triable.

DATED: February 23, 2015

Respectfully submitted,

PRITZKER LEVINE LLP

By: /s/ *Jonathan K. Levine*
Jonathan K. Levine (SBN: 220289)

Elizabeth C. Pritzker (SBN: 146267)
Shiho Yamamoto (SBN: 264741)
180 Grand Avenue, Suite 1390
Oakland, California 94612
Telephone: (415) 692-0772
Facsimile: (415) 366-6110
Email: jkl@pritzkerlevine.com;
ecp@pritzkerlevine.com
sy@pritzkerlevine.com

John A. Kehoe
41 Madison Avenue, 31st Floor
New York, New York 10010
Telephone: (917) 525-2190
Facsimile: (917) 525-2184
Email: jak@pritzkerlevine.com

Attorneys for Plaintiff Sterling International Consulting Group