UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

[UNDER SEAL],	)	Case No.
	)	
Plaintiffs,	)	COMPLAINT
	)	
vs.	)	
	)	
[UNDER SEAL],	)	**FILED IN CAMERA AND UNDER SEAL**
	)	**PURSUANT TO 31 U.S.C. § 3730(b)(2)**
Defendant.	)	
	)	

DOCUMENT TO BE KEPT UNDER SEAL

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, and the STATES OF CALIFORNIA, DELAWARE, FLORIDA, HAWAII, ILLINOIS, INDIANA, MASSACHUSETTS, MINNESOTA, MONTANA, NEVADA, NEW HAMPSHIRE, NEW JERSEY, NEW MEXICO, NEW YORK, NORTH CAROLINA, RHODE ISLAND, TENNESSEE, VIRGINIA and the DISTRICT OF COLUMBIA, ex rel. JAMES GLENN, Plaintiffs, vs. CISCO SYSTEMS, INC. Defendant.	)	Case No. COMPLAINT FOR VIOLATION OF THE FEDERAL FALSE CLAIMS ACT [31 U.S.C. § 3729 et seq.] and the FALSE CLAIMS ACTS of CALIFORNIA, DELAWARE, FLORIDA, HAWAII, ILLINOIS, INDIANA, MASSACHUSETTS, MINNESOTA, MONTANA, NEVADA, NEW HAMPSHIRE, NEW JERSEY, NEW MEXICO, NEW YORK, NORTH CAROLINA, RHODE ISLAND, TENNESSEE, VIRGINIA and the DISTRICT OF COLUMBIA **JURY TRIAL DEMANDED** **FILED IN CAMERA AND UNDER SEAL**

Plaintiff-Relator James Glenn ("Relator"), through his attorneys Phillips & Cohen LLP and Personius Melber LLP, on behalf of the United States of America, the States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Massachusetts, Minnesota, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Rhode Island, Tennessee, Virginia and the District of Columbia (collectively "the Plaintiff States"), for their Complaint against defendant Cisco Systems, Inc. ("Cisco"), alleges, based upon personal knowledge, relevant documents, and information and belief, as follows:

I. INTRODUCTION

1. This is an action to recover damages and civil penalties on behalf of the United States of America and the Plaintiff States arising from false and/or fraudulent statements, records, and claims made and caused to be made by defendant and/or its agents, employees and

co-conspirators in violation of the federal False Claims Act, 31 U.S.C. § 3729 et seq. (the "Act" or "FCA"), and the False Claims Acts of the Plaintiff States.

2. This qui tam case is brought against Defendant for selling and causing others to sell to federal agencies as well as to state and local government entities a video surveillance system that Defendant knew to possess dangerous, undisclosed, and impermissible security weaknesses.

3. Cisco manufactures and sells, inter alia, computer networking, voice, and communications technology and services. Among these products is the Video Surveillance Manager package of products, which is intended to control video surveillance cameras and to store and allow the manipulation of video created by the cameras. The Video Surveillance Manager is in turn comprised of three pieces of software: Cisco Video Surveillance Media Server, Cisco Video Surveillance Operations Manager, and Cisco Video Surveillance Virtual Matrix (collectively hereafter as Cisco's "Video Surveillance Manager" or "VSM").

4. Cisco is a large and established player in the video surveillance market, and touts itself as a "trusted advisor and networked physical security user" while asserting that "[w]ith deployments in transportation, airports, military, education, municipalities, retail, and more, the Cisco Video Surveillance Manager products meet[] the uncompromising needs of today's safety and security professionals."

5. Unfortunately for purchasers of the Video Surveillance Manager, the product is anything but secure. In fact, it has several critical security flaws. These flaws are so severe that they not only render the VSM product fatally insecure, but also compromise the security of any other computer or system connected to the VSM product.

6. Cisco markets the product as particularly suited for government customers, and knows that the product is routinely sold to government customers, even though Cisco knows that these critical security flaws render the product largely ineligible for purchase by government entities.

7. Moreover, although Cisco has known of these critical security flaws for at least two and a half years, it has failed to notify the government entities that have purchased and continue to use VSM of the vulnerability. Instead, Cisco continues to sell and cause others to sell this dangerous product to the United States and the Plaintiff States. Cisco's failure to inform its customers of these critical flaws is exacerbated by the fact that many of these customers pay an ongoing fee for Cisco premium services that promise to inform the customer of any known security issues or threats.

8. Defendant's conduct alleged herein violates the federal False Claims Act and the False Claims Acts of the Plaintiff States. The federal False Claims Act ("FCA") was originally enacted during the Civil War. Congress substantially amended the Act in 1986 – and, again, in 2009 and 2010 – to enhance the ability of the United States Government to recover losses sustained as a result of fraud against it. The Act was amended after Congress found that fraud in federal programs was pervasive and that the Act, which Congress characterized as the primary tool for combating government fraud, was in need of modernization. Congress intended that the amendments would create incentives for individuals with knowledge of fraud against the Government to disclose the information without fear of reprisals or Government inaction, and to encourage the private bar to commit legal resources to prosecuting fraud on the Government's behalf.

9. The FCA prohibits: (a) knowingly presenting (or causing to be presented) to the

federal government a false or fraudulent claim for payment or approval; (b) knowingly making or using, or causing to be made or used, a false or fraudulent record or statement material to a false or fraudulent claim; (c) knowingly making, using, or causing to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay or transmit money or property to the Government; and (d) conspiring to engage in any of the activities set forth in (a) through (c), above. 31 U.S.C. §§ 3729(a)(1)(A)-(C) and (G). Any person who violates the FCA is liable for a civil penalty of up to $11,000 for each violation, plus three times the amount of the damages sustained by the United States. 31 U.S.C. § 3729(a)(1).

10. The FCA allows any person having information about an FCA violation to bring an action on behalf of the United States, known as a qui tam suit, and to share in any recovery. The FCA requires that the qui tam Complaint be filed under seal and remain under seal for a minimum of 60 days (without service on the defendant during that time) to allow the Government time to conduct its own investigation and to determine whether to join the suit.

11. The Cisco Video Surveillance Manager is of no value to the Government because it fails to meet its primary purpose: enhancing the security of the agencies that purchase it. In many cases, the surveillance manager is actually detrimental to the purchaser because it eliminates or reduces the protection provided by other security systems. Notwithstanding the useless and potentially harmful nature of the product, Cisco continues to sell and cause others to sell the VSM to federal and state purchasers.

12. Because the VSM is a worthless (and even harmful) product, any claims Defendant submitted, or caused others to submit, to the United States or the Plaintiff States are false claims within the meaning of the federal and Plaintiff States' False Claims Acts.

13. In addition, as discussed in greater detail below, Cisco knows, within the meaning of the federal and Plaintiff States' False Claims Acts, that federal and many state government entities cannot purchase the VSM because the product, due to its critical security flaws, fails to comply with the security standards imposed on government systems by the Federal Information Security Management Act. Cisco, nonetheless, sells or causes others to sell the product to federal and state agencies while failing to inform government purchasers of these critical security flaws or of VSM's non-compliance with government standards.

14. And claims for VSM products, caused by Cisco's explicit and implicit representations about the security features of the product, and the product's compliance with federal or state information security standards, are false claims within the meaning of the federal and Plaintiff States' False Claims Acts.

15. Moreover, under the terms of some if not all of their contracts with the federal government and Plaintiff States, Defendant had a duty to repair or replace equipment that it knew to be flawed or faulty. By failing to make such repairs, Defendant knowingly avoided an obligation to pay money or transfer property to the federal and state governments.

16. Furthermore, Cisco sells a Security Posture Assessment service to many of its federal clients which purports to identify security vulnerabilities in the clients' networks. Any claims for this service package to entities using VSM products are false because Cisco has failed to disclose the vulnerability created by its own video surveillance systems and thus the product is worthless to the government.

17. Defendant has also conspired with other parties, including among others Relator's former employer NetDesign, to conceal the defects in the VSM products, and otherwise to facilitate knowingly selling to numerous government customers a worthless and harmful product.

18. As set forth below, Defendant's actions alleged in this Complaint also violate the California False Claims Act, Cal. Govt. Code § 12650 et seq.; the Delaware False Claims and False Reporting Act, 6 Del. C. § 1201 et seq.; the Florida False Claims Act, Fla. Stat. Ann. § 68.081 et seq.; the Hawaii False Claims Act, Haw. Rev. Stat. § 661-21 et seq.; the Illinois Whistleblower Reward and Protection Act, 740 Ill. Comp. Stat. § 175/1-8; the Indiana False Claims and Whistleblower Protection Act, Ind. Code § 5-11-5.5 et seq.; the Massachusetts False Claims Law, Mass. Gen. Laws ch. 12 § 5 et seq.; the Minnesota False Claims Act, Minn. Stat. § 15C.01 et seq.; Montana False Claims Act, Title 17, Ch. 8, Part 4, §§ 17-8-401 et seq.; the Nevada False Claims Act, Nev. Rev. Stat. Ann. § 357.010 et seq.; the New Hampshire False Claims Act, N.H. Rev. Stat. Ann. § 167:61 et seq.; the New Jersey False Claims Act, N.J. Stat. § 2A:32C-1 et seq.; the New Mexico Fraud Against Taxpayers Act, N.M. Stat. Ann. § 44-9-3 et seq.; the New York False Claims Act, N.Y. State Fin. § 187 et seq.; the North Carolina False Claims Act, N.C. Gen. Stat. § 1-605 et seq.; the Rhode Island False Claims Act, R.I. Gen. Laws § 9-1.1-1 et seq.; the Tennessee False Claims Act, Tenn. Code Ann. § 4-18-101 et seq.; the Virginia Fraud Against Taxpayers Act, Va. Code Ann. § 8.01-216.1 et seq.; and the District of Columbia Procurement Reform Amendment Act, D.C. Code Ann. § 1-1188.13 et seq.

19. Based on these provisions, qui tam plaintiff and relator James Glenn seeks to recover all available damages, civil penalties, and other relief for the federal and state-law violations alleged herein.

II. PARTIES

20. Plaintiff/Relator James Glenn is a United States citizen, currently residing in Copenhagen, Denmark. He has more than 10 years of experience in the computer networking and security industry. In March 2007, he began working for the Managed Security Division of Tele-Denmark Communications ("TDC"), a Danish communications services company. In July of 2007, Relator's division was acquired by NetDesign, another Danish network services provider. Mr. Glenn worked on security issues at NetDesign until March of 2009, when, as set forth in greater detail below, he was fired for reporting Cisco's security violations. Mr. Glenn currently works for Milestone Systems, a market leader in video surveillance software, as a software support engineer.

21. Defendant Cisco Systems, Inc. is a California corporation with its headquarters in San Jose, California. In 2010, Cisco had over $40 billion in total sales. Cisco is one of the nation's largest information technology ("IT") services providers and has a growing presence in the security software field. Cisco aggressively markets its security, and other, products to government purchasers, including agencies of the United States and the Plaintiff States.

III. JURISDICTION AND VENUE

22. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1367, and 31 U.S.C. § 3732, the last of which specifically confers jurisdiction on this Court for actions brought pursuant to 31 U.S.C. §§ 3729 and 3730. In addition, 31 U.S.C. § 3732(b) specifically confers jurisdiction on this Court over the State law claims.

23. Under 31 U.S.C. § 3730(e) and the comparable provisions of the Plaintiff States' False Claims Acts, there has been no statutorily relevant public disclosure of the "allegations or

transactions" in this case. Relator, moreover, would qualify under those provisions as an "original source" of the allegations in this Complaint even had such a public disclosure occurred. To the extent that there could have been a public disclosure under 31 U.S.C. § 3732(e)(4)(A), Relator possesses information that is independent of and materially adds to any potentially publicly disclosed allegations. Relator has also voluntarily provided information about Cisco's violations to the Government before filing this action.

24. This Court has personal jurisdiction over the Defendant pursuant to 31 U.S.C. § 3732(a), which authorizes nationwide service of process and because Defendant has minimum contacts with the United States, and can be found in and/or transacts business in this District.

25. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and 1395(a) and 31 U.S.C. § 3732(a) because Defendant can be found in and/or transacts business in this District. At all times relevant to this Complaint, Defendant regularly conducted substantial business within this District, maintained employees in this District, and/or made significant sales within this District. In addition, statutory violations, as alleged herein, occurred in this District.

IV. APPLICABLE LAW

A. Federal Acquisition Regulation

26. The Federal Acquisition Regulations ("FAR"), codified in Title 48 of the United States Code of Federal Regulations ("CFR"), govern the federal procurement process from need recognition and acquisition planning through contract formation, and contract administration.

27. The FAR was amended on September 30, 2005 "to implement the information technology security provisions of the Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Government Act of 2002 (E-Gov Act))." 70 FR 57449, 57450 (2005) finalized without substantive change 71 FR 57360 (2006). The motivation for and

purpose of the FISMA and the implementing provisions were explained as follows:

> American society relies on the Federal Government for essential information and services provided through interconnected computer systems. Both Government and industry face increasing security threats to essential services and must work in close partnership to address those risks. Increasingly, contractors are supplying, operating, and accessing critical IT systems, performing critical functions throughout the life of IT systems. At the same time, it is apparent that information technology and the IT marketplace have become truly global. The security risks are shared globally as well.
>
> Unauthorized disclosure, corruption, theft, or denial of IT resources have the potential to disrupt agency operations and could have financial, legal, human safety, personal privacy, and public confidence impacts. The Federal community has not focused on unclassified activities with regard to information technology resources involved in the acquisition and use of information on behalf of the Government. In particular, there is need to focus on the role of contractors in security as more and more Federal agencies outsource various information technology functions. Until now, regulations have generally been silent regarding security requirements for contractors who provide goods and services with IT security implications.
>
> This rule amends FAR parts 1, 2, 7, 11, and 39 to implement the information technology security provisions of the Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Government Act of 2002 (EGov Act)). The rule recognizes security as an important part of all phases of the IT acquisition life cycle. The rule focuses much needed attention on the importance of system and data security by contracting officials and other members of the acquisition team.
>
> The intent of adding specific guidance in the FAR is to provide clear, consistent guidance to acquisition officials and program managers; and to encourage and strengthen communication with IT security officials, chief information officers, and other affected parties.

Id. (emphasis added).

28. To accommodate the growth, change and evolution of the information technology products and services to be purchased by the Government, the FAR incorporates external standards – the Federal Information Processing Standards ("FIPS") – rather than trying to create a separate standard. See id.

29. Accordingly, 48 C.F.R. § 11.102 requires agencies to adhere to the FIPS when

purchasing information technology systems. Federal agencies cannot purchase information technology systems that do not comply with the FIPS.

B. Federal Information Processing Standards

30. FISMA gave the Department of Commerce the mandate to set security and data processing standards for all non-classified federal information technology initiatives. The Department of Commerce in turn delegated its responsibilities to the National Institute of Science and Technology ("NIST"). NIST formed a FISMA Implementation Committee in 2003, which promulgates two sets of documents: Federal Information Processing Standards ("FIPS") and Special Publications ("SP").

31. Because the FIPS are mandatory, the NIST followed rules similar to those in the Administrative Procedure Act before implementing each new standard, namely: publication in the Federal Register, public comment, justification, and then approval by the Secretary of Commerce.

32. The SPs are submitted for public comment but do not, in and of themselves, have the force of law. They are also more numerous than the FIPS. However, the SPs serve to highlight important security concerns facing public agencies and propose recommended solutions and best practices for information management.

33. Furthermore, the FIPS often incorporate SPs by reference, thereby making recommended policies binding on government agencies.

34. One of the most important SPs is SP 800-53 rev. 3 "Recommended Security Controls for Federal Information Systems and Organizations" (Aug. 2009). SP 800-53 rev. 3 is incorporated into FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems" (Mar. 2006). See FIPS 200 at iv ("Federal agencies must meet the

minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended.")

35. Therefore, any and all recommended controls contained in SP 800-53 are binding on government agencies and government agencies may not procure, install, or maintain systems that do not comply with SP 800-53 and FIPS 200.

36. SP 800-53 is divided into various categories of security measures, including Access Controls ("AC"), Audit and Accountability ("AU"), Identification and Authentication ("IA"), and System and Communications Protection ("SP"). Within each category, there are many numbered mandates (e.g., AC-1, SP-7, etc.) laying out particular requirements in detail.

37. As outlined in greater detail below Cisco's VSM violates many of the SP 800-53 requirements, including, inter alia: AC-3 ("Access Control Enforcement"); AC-6 ("Least Privilege"); IA-5 ("Authenticator Management"); SC-8 ("Transmission Integrity"); SC-9 ("Transmission Confidentiality"); SC-23 ("Session Authenticity"); SC-28 ("Protection of Information at Rest"); and SI-10 ("Information Input Validation").

38. FIPS 200 makes no provision for waiver of its requirements. Id. at v ("No provision is provided under FISMA for waivers to FIPS made mandatory by the Secretary of Commerce."). Had federal purchasers been aware of the defects in the Cisco VSM, they would have been unable to purchase it, because their information technology security would not have been compliant with FIPS 200 or SP 800-53. Id. at iv.

V. BACKGROUND

A. Cisco Sales Structure

39. While Cisco does sell certain of its products directly to business users, it generally offers them to the market through affiliated distributors, which it refers to as "Cisco Partners."

These Partners sell the Cisco products to the ultimate customers on Cisco's behalf, often bundled with video surveillance cameras, computer equipment and other hardware.

40. Cisco represents to its customers that it selects it's Cisco Partners based on their expertise in certain product areas, such as "Unified Communications" or "Managed Connectivity." Cisco claims that it carefully selects and trains its partners, exercising substantial control over their technical expertise and approach to selling Cisco products. Cisco then uses this close relationship with its partners as a selling feature when pitching Cisco products to potential customers. Cisco markets its "Partners" to its customers as "trusted advisor[s] who ha[ve] the technology breadth to deliver integrated network solutions, and the technology depth to deliver highly specialized solutions." See http://www.cisco.com/web/partners/downloads/765/tools/ quickreference/cust_br.pdf (visited March 28, 2011).

41. Although the Cisco Partners ultimately sell and install the Cisco products, Cisco itself markets its products directly to government purchasers, and works hand-in-hand with its Partners in this process. Cisco's web site, for example, provides extensive guidance for federal and state agencies looking to buy Cisco products, including detailed case studies, technical specifications analysis and testimonials from other government agencies or customers who have purchased Cisco's products.

42. Cisco then points the potential Government customer to one or more Cisco Partners for the ultimate sale, installation and servicing of the Cisco product. For example, at http://www.cisco.com/web/strategy/government/usfed_contracts.html (visited March 28, 2011), Cisco's web site identifies a variety of federal and/or state purchasing options, and directs the

potential government customer to different lists of Cisco Partners depending on the type of program at issue:

> Federal procurement requires that purchasers navigate a complex process. Cisco offers a number of avenues and programs to assist agencies with the federal procurement process for Cisco products and services.
>
> Cisco works with a number of industry partners to offer a wide variety of products and services through government contracting vehicles. Please refer to the individual contract to learn its specific details, view ordering information, and see the lists of Cisco products offered for federal procurement on that contract. Contracts include:
>
> - COMMITS NexGen: COMMITS NexGen is an ID/IQ task order contract for IT solutions and is available to any federal agency.
> - ESC III: ECS III offers products and services for desktop computing, LAN/WAN infrastructure, and UNIX needs.
> - FirstSource: FirstSource provides access to IT commodity products for DHS and any agency working on DHS-related programs.
> - GSA: The GSA Schedules program establishes long-term, government-wide contracts for commercial supplies and services.
> - NETCENTS: NETCENTS is a U.S. Air Force ID/IQ contract for technologies and services and is available to all federal agencies.
> - Networx: Networx is a GSA program to provide all federal agencies with comprehensive, best-value telecommunications, networking services, and technical solutions.
> - SEWP: The NASA SEWP government-wide acquisition contract provides the latest in IT products for all federal agencies.
> - VETS GWAC: VETS GWAC is a small business set-aside contract for service-disabled veteran-owned small businesses.

43. Accordingly, Cisco is not only aware that its products – including the VSM product – are sold to Government purchasers, Cisco also actively promotes such sales.

B. Product Overview

44. In 2007, Defendant Cisco purchased BroadWare, a provider of Internet Protocol ("IP") based video surveillance software. Cisco then adapted BroadWare's products to create its own IP video surveillance product: the Cisco Video Surveillance Manager.

45. The Video Surveillance Manager is in turn made up of three primary components: the Cisco Video Surveillance Media Server ("VSMS"), the Cisco Video Surveillance Operations Manager ("VSOM"), and the Cisco Video Surveillance Virtual Matrix ("VSVM") (collectively "Video Surveillance Manager" or "VSM"). The three parts of the system may be purchased separately, but Cisco markets them as a joint package.

46. In conjunction, these products allow for the connection and management of multiple video cameras through a centralized server, which can in turn be accessed remotely. In other words, the VSM can connect camera systems from around the country and consolidate the storage of data and allocation of video streams in one (or a few) primary locations. The Cisco VSM is particularly useful for organizations wishing to coordinate camera surveillance over multiple physical locations (e.g., a federal agency with dozens of office buildings to monitor).

47. The VSMS is the core component of the Video Surveillance Manager, collecting and routing video from cameras to viewers or other media servers. It can support anywhere from a few cameras in one building to hundreds of video feeds across the country.

48. The VSOM server software controls access to the IP surveillance system (i.e., the cameras). Users are assigned "roles" which determine which video feeds they are able to view. The VSOM is responsible for presenting camera feeds, video archives, and predefined views to the viewer. Once this information is provided to the viewer, the viewer communicates with the appropriate media server (usually the VSMS) to request and receive video streams.

49. The VSVM is responsible for providing monitor layout information to video system user monitors. Once the monitor layout and views are sent to the monitors, the monitors are responsible for contacting the appropriate Media Server(s) to request video streams. In other words, the VSVM is responsible for coordinating and formatting the video display of users (e.g.,

at a control center) who view multiple video streams at once.

50. On the commercial market, a single license for the VSOM costs approximately $5,000, a license for the VSMS around $500, and a license for the VSVM approximately $400. They are also often sold with Cisco's own IP video cameras, which cost around $700 each.

51. The Cisco VSM has been on the market since 2008, when Cisco completed its adaptation of the technology that it purchased from BroadWare in 2007. The security flaws discussed herein were present in the original BroadWare software and Cisco did not correct them otherwise modify the VSM following its purchase of BroadWare technology.

VI. ALLEGATIONS

52. Cisco is a large and established player in the video surveillance market, proclaiming its status as a "trusted advisor and networked physical security user" and asserting that "[w]ith deployments in transportation, airports, military, education, municipalities, retail, and more, the Cisco Video Surveillance Manager products meet[] the uncompromising needs of today's safety and security professionals."

53. Unfortunately for purchasers of the Video Surveillance Manager, it is anything but secure. In fact, the VSM has several critical security flaws that violate the mandatory technical requirements imposed on any computer system sold to the Government including: enforcement of access control, prevention of information leakage through use of encryption, proper validation of control requests, and confirmation of inputs from external or untrusted sources. NIST Special Publication 800-53 revision 3, AC-3; AC-6; IA-5; SC-8; SC-9; SC-23; SC-28; SI-10.

54. As a result of these defects, a person with a moderate knowledge of software / network security and the Cisco VSM could exploit the system in a number of ways, including: gaining access to all video feeds, gaining access to all user passwords, gaining access to all

stored data on the system, modifying or deleting video feeds, and gaining permanent "administrator" (i.e., highest-level) access to the system (which would enable future abuse to go completely undetected).

55. Defendant has been aware of these issues since at least October 2008, when Relator submitted a detailed report to Cisco showing that the Cisco VSM needed to be overhauled or withdrawn from the market. Relator was fired shortly after disclosing his concerns to Cisco and his employer (one of Cisco's Danish distributors).

56. To Relator's knowledge, Defendant has never publicly disclosed these vulnerabilities or privately disclosed them to Government or other purchasers. Defendant has also not patched or otherwise modified the Cisco VSM to correct these flaws. Instead, Cisco continues to fraudulently market the VSM as a secure and reliable tool to federal and state agencies, many of which have critical security needs.

A. Cisco's Video Surveillance Manager Contains Security Flaws Which Render the Product Worthless

57. The Cisco VSM is fundamentally flawed leading it to create significant security flaws in any system into which it is incorporated. These flaws are so significant that it would be difficult to correct them sufficiently to bring the product into compliance with federal purchasing standards, even if Cisco fully disclosed the flaws to government purchasers. Because Cisco has deliberately refused to disclose these flaws to government purchasers, the vast majority of all such systems sold to government customers remain in their vulnerable state – a wide network of security disasters waiting to happen.

58. For security purposes, this complaint will not describe the full technical details of these flaws. Instead, the flaws will be described only in general terms, focusing primarily on their effect. A disk demonstrating these flaws and detailed technical report are being provided to

the Government as part of the statutory disclosure materials.

59. The most critical flaw in the Cisco VSM allows the user of any video observation point, no matter how restricted, to gain access to the full contents of the system to which the central server is connected. This vulnerability has three grave consequences.

60. First, the flaw may compromise an entity's entire computer system. Many of Cisco's customers have the surveillance system's central media server installed on a computer that is connected to the same Local Area Network (LAN) as the rest of their computers. Due to the vulnerability in Cisco's surveillance system, any user who has or can gain access to one video camera could potentially gain unauthorized access to the entire network of a federal agency.

61. This unauthorized access could even allow the intruder to take control of or bypass the entity's "physical security" systems (e.g., locks, fire alarms, access panels, etc.) because these systems are regularly connected to the camera system so that video may be triggered by an emergency.

62. Second, the Cisco VSM allows for any user at one location to observe all video feeds recorded on the central media server. Thus, an individual authorized to view one video feed could observe, as well as modify or disable, all of the video feeds tied in to the central media server. This flaw creates obvious physical security risks to any facility protected by the Cisco VSM.

63. Third, the vulnerability created by the Cisco VSM also allows an unauthorized user to gain the highest level of access (generally described as "admin" or "administrator" access) to the compromised system without any record created showing that the user has such access. This would enable the unauthorized user to modify key aspects of the system, access any

data on the system, or make use of its functions, at any point following the initial breach. The unauthorized user could also obtain the passwords of all authorized users and then log on as any of them at a future point in time.

64. Thus, for example, an unauthorized user could effectively shut down an entire airport by taking control of all security cameras and turning them off. Alternately, such a hacker could access the video archives of a large entity to obscure or eliminate video evidence of theft or espionage. Even more, such a hacker could use his or her access to the system (gained through the vulnerabilities created by the VSOM) to gain physical access to a supposedly secure facility if the key-card reader and other security features were connected to the same server as the VSOM.

65. Cisco knows that the flaws in its Video Surveillance Manager are unlikely to be detected by many purchasers because of the nature of the market for video surveillance systems. In general, such systems are marketed to and purchased by the "physical" security division of most organizations. Physical security departments generally focus on traditional "badge and gun" security, and tend to be less familiar with computer security issues, which are typically handled by an organization's IT personnel. In Relator's experience, IT security personnel regard their work as distinct from the "physical" security issues in a building, and thus are not as likely to check a product like the Video Surveillance Manager for FIPS violations or other security flaws.

66. Cisco understands the risks of segregating physical and IT security functions first hand. In 2001, Cisco's computer networks – including its security networks – were compromised by a virus that infiltrated the system by using vulnerabilities in the company's video surveillance systems. At the time, Cisco identified the segregation of its physical and IT

security functions as one of the reasons the security vulnerability was not identified before the virus hit.

67. Gaining the unauthorized access described above does not require any special software or extraordinary technical knowledge. A party desiring to breach the system's security would only need to be aware of the vulnerabilities in Cisco's system – knowledge that could be gained through routine usage of the software – and have a basic degree of competency with computers and networking software.

B. The Significant Flaws in Cisco's Video Surveillance Manager Cause the Product To Violate Multiple Federal Information Processing Standards

68. As described above, the FIPS 200 Standard incorporates the SP 800-53 revision 3 recommendations into its mandatory requirements for federal contractors. As Cisco well knows, federal agencies, and any state agencies that rely on FIPS, cannot purchase systems that are not FIPS-compliant.

69. However, Cisco markets and sells (and causes others to sell) the product to government purchasers notwithstanding its knowledge that the significant flaws in the VMS product violate numerous FIPS requirements. Some of these standards include, inter alia, the standards identified in the following paragraphs.

70. Standard AC-3 ("Access Control Enforcement") requires that: "The information system enforces approved authorizations for logical access to the system." In violation of this standard, the Cisco VSM allows users to gain access to key system functions without authorization by failing to verify the user's "role" (i.e., authorized purpose for being in the system) before granting access to key control functions.

71. Standard AC-6 ("Least Privilege") requires that: "The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on

behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." In violation of this standard, the Cisco VSM allows users to obtain access to video feeds and other data far outside their authorized purpose for accessing the system.

72. Standard IA-5 ("Authenticator Management") requires the system to take a variety of steps to ensure that passwords or other confirmation such as biometrics are necessary to submit commands to the system. IA-5 further requires that the system takes steps to prevent the disclosure of these authenticators to unauthorized users. In violation of this standard, the Cisco VSM allows unauthorized access to a system wide password list and also fails to require adequate authentication before allowing access to sensitive system areas.

73. Standard SC-8 ("Transmission Integrity") requires that: "The information system protects the integrity of transmitted information." In violation of this standard, the Cisco VSM allows users to gain access to video servers and corrupt, modify, or delete video feeds they are not authorized to view or access.

74. Standard SC-9 ("Transmission Confidentiality") requires that: "The information system protects the confidentiality of transmitted information." In violation of this standard, the Cisco VSM allows unauthorized modification or reproduction of videos and fails to use encryption to properly protect the contents of the videos.

75. Standard SC-23 ("Session Authenticity") requires that: "The information system provides mechanisms to protect the authenticity of communications sessions." This is a macro level version of AC-3, in that it imposes a duty on the system to ensure an authentic user at the session, or initial level, as well as for each piece of data transmitted. In violation of this standard, if compromised, the Cisco VSM could allow an unauthorized user to log in as any

legitimate user, or without providing any login information.

76. Standard SC-28 ("Protection of Information at Rest") requires that: "The information system protects the confidentiality and integrity of information at rest." In violation of this standard, the Cisco VSM presents ample opportunity for the disclosure or modification of any and all video data stored in its archives.

77. Standard SI-10 ("Information Input Validation") requires that: "The information system checks the validity of information inputs." This rule is designed to ensure that the system properly processes data inputs as information and not as a command. In other words, the system should draw a line between its command functions and its data-entry functions. In violation of this standard, the Cisco VSM has inadequate protection on this front, which allows for forcible access to its control functions by sending commands to what should be information-only ports.

C. Cisco Security Posture Assessment

78. To add insult to injury, Cisco also offers its customers an additional service called the Cisco Security Posture Assessment, which purports to provide "a detailed assessment of network devices, servers, desktops, web applications, related IT infrastructure elements such as physical facilities, and operation security management" with the objective of "protect[ing] critical federal IT infrastructure from both physical and cyber security intrusions."

79. The Security Posture Assessment is marketed to government purchasers as a comprehensive evaluation of any and all security vulnerabilities in their IT software and hardware. Relator believes, and on this basis alleges, that many federal and state agencies that purchased the Cisco VSM also purchased the Security Posture Assessment.

80. Because Relator has seen no public reports from Cisco or elsewhere about this vulnerability, he believes, and on this basis alleges, that Cisco has not notified any of these

agencies of the vulnerability created by its own product, nor taken any other steps to remedy this grave violation of its obligations to purchasers of the Security Posture Assessment.

81. When a vulnerability of this magnitude is identified, news of the issue is generally circulated to all purchasers of a product, so that the flaw may be quickly corrected. After a sufficient period of time has passed to allow purchasers to make repairs, the company will also publish the vulnerability and, if appropriate, credit any external entity that discovered the flaw. Cisco has made no such publication describing the vulnerability in its VSM system.

D. Relator's Discovery and Reports to Cisco of the Problems with the Video Surveillance Manager

82. Relator discovered the flaws in Cisco's VSM while working at NetDesign, a Danish networking company that is also a Cisco "Gold Certified" Partner. At NetDesign, Relator worked on a variety of security projects for various clients, some involving Cisco products. Among other tasks, he worked on network security for the Danish National Police ("Rigspolitet") and the Copenhagen County Police Department.

83. Relator eventually discovered the flaw in the Cisco VSM not through a specific work assignment, but through NetDesign's "Own Medicine" program. The Own Medicine program encouraged NetDesign's employees to test the software and systems the company itself used, to try to discover vulnerabilities and problems.

84. In September of 2008, Relator and a colleague who worked in NetDesign's "physical security" department were testing an Internet-based Cisco security camera, looking for problems and vulnerabilities. Relator's colleague discovered that the camera (and related software) did not log failed attempts to access it, thus making the camera and system highly vulnerable to "brute force" security breaches (i.e., repetitive attempts to guess the password). Relator then reported his colleague's discovery to Cisco on October 30, 2008. Cisco issued a

patch and notice of the problem in the next update to the software.

85. Relator took his colleague's achievement as a challenge and decided he would find a comparable security flaw. Having recently worked on the Cisco Video Surveillance Manager for other projects, Relator began experimenting with it to locate defects in its security structure.

86. Once he began to work with the product, he realized his challenge was much easier than he had anticipated – the Video Surveillance Manager was riddled with serious security defects. Relator made the discovery at the heart of these allegations in October of 2008 and spent a few weeks testing and confirming that his concerns were valid. In late October, he presented the vulnerabilities, with evidence, to his supervisor, Karsten Frantsen. Frantsen expressed concern about the issue, but gave no indication that he planned to act on the information.

87. At the same time he talked to Frantsen, Relator also submitted a report on the vulnerability to Cisco, through the company's Product Security Incident Response Team (PSIRT). Relator included a detailed description of the problem, including screenshots demonstrating that he had breached a test media server through various connected cameras. Relator did not receive any response from Cisco to this submission other than an automated notice that it had been received.

88. In November of 2008, Relator followed up his PSIRT submission by writing a personal letter to the Cisco Incident Manager named on the automated PSIRT response. The manager wrote back to Relator with a pro forma response that indicated he would be "working with" Relator to resolve the issue. After a few more inquiries from Relator, the Incident Manager simply told him that there was "no quick fix" to resolve the problem and did not further

reply.

89. On November 25, 2008, Relator was invited by Frantsen to join a December 2 conference call between Cisco representatives and NetDesign about the flaws in the Cisco VSM. Relator did not keep notes of the call and thus does not have the names of the Cisco representatives he spoke with. During the course of the call, Relator and the colleague who helped him discover the vulnerability explained the security issue to Cisco in technical detail. The Cisco representatives asked Relator if he had any suggestions on how to fix the software. Relator indicated his belief that the problem was intrinsic to the design and structure of the Cisco VSM and largely irreparable.

90. After the conference call, in December, Relator continued to discuss his concerns about the Cisco system with Frantsen and expressed his opinion that NetDesign should not offer the Cisco VSM to its clients.

91. On March 3rd, Relator received a forwarded message from his colleague indicating that Brent Cowing of Cisco would be meeting with Frantsen and other NetDesign representatives at 8:30 PM that day. Relator took that opportunity to remind Frantsen by e-mail that vulnerabilities were still present in the system.

92. For reasons Relator is not aware of, the 8:30 PM meeting did not take place. However, at 8:47 PM on March 3rd, Relator received an Outlook calendar invitation from Frantsen for a March 9 meeting regarding Cisco. Frantsen made no response to Relator's e-mail regarding the problems with the system.

93. Cisco representatives arrived at NetDesign on March 6 and met with Frantsen and other NetDesign employees. Relator was not invited to this meeting, nor was he informed about what was discussed at the meeting.

94. On March 9, Relator was called into Frantsen's office, where other NetDesign managers were present, and dismissed from his position with the company. He was told that his firing was due to economic concerns, even though the company had recently completed a record year. Moreover, at the time Relator had a full workload, including several projects that no other NetDesign employee was in a position to take over.

95. Based on the circumstances of his firing, Relator believes, and on that basis alleges, that he was fired in retaliation for alerting Cisco and NetDesign to the flaws in the Cisco VSM product.

96. After he was fired, Relator continued to monitor Cisco's public pronouncements about its Video surveillance system, hoping to see that Cisco had fixed the problem or at least informed its customers of the vulnerability. During this period he was also dealing with certain unrelated health issues.

97. Finally, hearing nothing from Cisco, and confirming that the problem with the system had not been fixed, in September of 2010 Relator asked a trusted family member to call FBI headquarters and express concern about the fact that the Cisco VSM is installed at Los Angeles International Airport. The relative's inquiries were forwarded along to Detective Edward Martinez of the Los Angeles Airport Police, who then called and spoke with Relator. Detective Martinez is a member of the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Force. Relator provided Detective Martinez with the same photographic and documentary evidence of the flaw that he had previously given to Cisco.

E. Government Purchasers of Cisco Video Surveillance Manager

98. As noted above, Cisco has sold the Cisco VSM, either directly or indirectly, to federal, state, and local government agencies both large and small. Some examples of sales in

this District include the following:

99. In 2009, the United States Department of Homeland Security awarded the Albion, NY Police Department a grant to purchase a SightLogix brand "rapid deployment kit," consisting of Cisco video cameras and a Panasonic laptop running the Cisco VSM. The grant was made under the Department's Commercial Equipment Direct Assistance Program.

100. In addition, Amtrak uses the Cisco VSM to provide security at its stations. On this basis, Relator alleges, on information and belief, that the Amtrak stations located in Buffalo, NY and Niagara Falls, NY are also equipped with the Cisco Video Surveillance Manager.

101. Relator is also aware that the following United States and United States-funded agencies and entities have purchased VSM, inter alia: the Department of Homeland Security, the Secret Service Procurement Division, the Department of Defense Biometrics Task Force Headquarters, the Federal Emergency Management Agency, the National Aeronautics and Space Administration (NASA), the Army, the Navy, the Air Force, the Marine Corps, and the Patent and Trademark Office.

102. Cisco aggressively markets the VSM to states and local governments, especially schools, courts, municipal offices and airports. Cisco prominently displays, on its web site, case studies of the VSM being used by such state and local government entities. Below are examples of some state and local entities known by Relator to have purchased or otherwise acquired Cisco VSM, often with Federal assistance and / or through the federal supply schedule. Based on Cisco's aggressive marketing to state and local entities Relator believes, and on that basis alleges, that each of the Plaintiff States have purchased the Cisco VSM product.

103. Even those entities that acquired the Video Surveillance System without spending their own money (e.g., through a Department of Homeland Security Grant) have been harmed by

the product if they have connected the product to any of their existing computer systems or networks, because the security flaws in the Cisco product damage the security of any other computer system to which it is connected.

104. California state and local agencies and entities that have purchased VSM include, inter alia: Alameda County Congestion Management Agency, California State University–Monterey Bay, City of Mission Viejo California, County of Santa Cruz – Sheriff-Coroner, Fort Bragg Unified School District, Grant Joint Union High School, Los Angeles International Airport, San Diego International Airport/San Diego County Regional Airport Authority, and San Joaquin County.

105. District of Columbia state and local agencies and entities that have purchased VSM include, inter alia: the Washington D.C. Metro Police Department, and the Woodrow Wilson Senior High School.

106. Illinois state and local agencies and entities that have purchased VSM include, inter alia: City of Joliet Police Department, Joliet Junior College, and Midway International Airport.

107. Massachusetts state and local agencies and entities that have purchased VSM include, inter alia: the Commonwealth of Massachusetts, Ashland Township, Beverly Township, Lawrence Township, and Westford Township.

108. New Jersey state and local agencies and entities that have purchased VSM include, inter alia: the State of New Jersey, and Livingston Public Schools.

109. New York state and local agencies and entities that have purchased VSM include, inter alia: Glen Cove School District, New York MTA, and State University of New York – SUNY Delhi.

110. Virginia state and local agencies and entities that have purchased VSM include, inter alia: the Fredericksburg Police Department.

Count I
Federal False Claims Act
31 U.S.C. §§ 3729(a)(1)(A)-(C), (G)

111. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

112. This is a claim for treble damages and penalties under the False Claims Act, 31 U.S.C. § 3729, et seq., as amended.

113. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the United States Government for payment or approval.

114. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

115. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the Government.

116. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

117. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false claims were presented by numerous separate entities,

across the United States. Relator has no control over or dealings with such entities and has no access to the records in their possession.

118. The Government, unaware of the falsity of the records, statements and claims made or caused to be made by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's illegal conduct.

119. By reason of Defendant's acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

120. Additionally, the United States is entitled to the maximum penalty of up to $11,000 for each and every violation alleged herein.

Count II
California False Claims Act
Cal Govt Code §§ 12651(a)(1)-(3), and (7)

121. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

122. This is a claim for treble damages and penalties under the California False Claims Act.

123. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

124. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

125. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or

transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

126. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

127. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

128. The California State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's illegal conduct.

129. By reason of Defendant's acts, the State of California has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

130. Additionally, the California State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count III
Delaware False Claims and Reporting Act
6 Del C. §§ 1201(a)(1)-(3), and (7)

131. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

132. This is a claim for treble damages and penalties under the Delaware False Claims and Reporting Act.

133. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

134. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

135. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

136. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

137. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

138. The Delaware State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's illegal conduct.

139. By reason of Defendant's acts, the State of Delaware has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

140. The State of Delaware is entitled to the maximum penalty of $11,000 for each and

every violation alleged herein.

Count IV
Florida False Claims Act
Fla. Stat. Ann. §§ 68.082(2)(a)-(c), and (g)

141. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

142. This is a claim for treble damages and penalties under the Florida False Claims Act.

143. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

144. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

145. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

146. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

147. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and

has no access to the records in their possession.

148. The Florida State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

149. By reason of Defendant's acts, the State of Florida has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

150. Additionally, the Florida State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count V
Hawaii False Claims to the State and to the Counties Acts
Haw. Rev. Stat. §§ 661-21(a)(1)-(3), and (7) and §§ 46-171(a)(1)-(3), and (7)

151. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

152. This is a claim for treble damages and penalties under the Hawaii False Claims to the State Act and Hawaii False Claims to the Counties Act.

153. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

154. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

155. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or

decreased an obligation to pay or transmit money to the State.

156. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

157. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

158. The Hawaii State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

159. By reason of Defendant's acts, the State of Hawaii has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

160. Additionally, the Hawaii State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count VI
Illinois Whistleblower Reward and Protection Act
740 Ill. Comp. Stat. §§ 175/3(a)(A)-(C), and (G)

161. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

162. This is a claim for treble damages and penalties under the Illinois Whistleblower Reward and Protection Act.

163. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related

services to the State for payment or approval.

164. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

165. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

166. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

167. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

168. The Illinois State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct..

169. By reason of Defendant's acts, the State of Illinois has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

170. Additionally, the Illinois State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count VII
Indiana False Claims and Whistleblower Protection Act
Ind. Code Ann. §§ 5-11-5.5-2(b)(1)-(2) and (6)-(7)

171. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

172. This is a claim for treble damages and penalties under the Indiana False Claims and Whistleblower Protection Act.

173. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

174. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

175. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

176. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

177. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

178. The Indiana State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

179. By reason of Defendant's acts, the State of Indiana has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

180. Additionally, the Indiana State Government is entitled to the maximum penalty of $5,000 for each and every violation alleged herein.

Count VIII
Massachusetts False Claims Law
Mass. Gen. Laws ch. 12 §§ 5B(1)-(3), and (8)

181. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

182. This is a claim for treble damages and penalties under the Massachusetts False Claims Law.

183. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

184. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

185. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

186. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

187. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

188. The Massachusetts State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

189. By reason of Defendant's acts, the State of Massachusetts has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

190. Additionally, the Massachusetts State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count IX
Minnesota False Claims Act
Minn. Stat. §§ 15C.02(a)(1)-(3), and (7)

191. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

192. This is a claim for treble damages and penalties under the Minnesota False Claims Act.

193. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related

services to the State for payment or approval.

194. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

195. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

196. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

197. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

198. The Minnesota State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

199. By reason of Defendant's acts, the State of Minnesota has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

200. Additionally, the Minnesota State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count X
Montana False Claims Act
Mont. Code Ann. §§ 17-8-403(1)(a)-(c), (g)

201. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

202. This is a claim for treble damages and penalties under the Montana False Claims Act.

203. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

204. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

205. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

206. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

207. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

208. The Montana State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

209. By reason of Defendant's acts, the State of Montana has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

210. Additionally, the Montana State Government is entitled to the maximum civil penalties of $10,000 for each and every violation alleged herein.

Count XI
Nevada False Claims Act
Nev. Rev. Stat. Ann. §§ 357.040(1)(a)-(c), and (g)

211. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

212. This is a claim for treble damages and penalties under the Nevada False Claims Act.

213. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

214. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

215. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

216. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

217. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

218. The Nevada State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

219. By reason of Defendant's acts, the State of Nevada has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

220. Additionally, the Nevada State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count XII
New Hampshire False Claims Act
N.H. Rev. Stat. Ann. §§ 167:61-b(I)(a)-(c), and (e)

221. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

222. This is a claim for treble damages and penalties under the New Hampshire False Claims Act.

223. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

224. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

225. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

226. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

227. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

228. The New Hampshire State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

229. By reason of Defendant's acts, the State of New Hampshire has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

230. Additionally, the New Hampshire State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count XIII
New Jersey False Claims Act
N.J. Stat. §§ 2A:32C-3(a)-(c) and (g)

231. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

232. This is a claim for treble damages and penalties under the New Jersey False Claims for Medical Assistance Act.

233. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

234. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

235. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

236. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

237. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

238. The New Jersey State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

239. By reason of Defendant's acts, the State of New Jersey has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

240. Additionally, the New Jersey State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count XIV
New Mexico Fraud Against Taxpayers Act
N.M. Stat. Ann. § 44-9-3

241. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

242. This is a claim for treble damages and penalties under the New Mexico Fraud Against Taxpayers Act.

243. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

244. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

245. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or

decreased an obligation to pay or transmit money to the State.

246. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

247. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

248. The New Mexico State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

249. By reason of Defendant's acts, the State of New Mexico has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

250. Additionally, the New Mexico State Government is entitled to the maximum civil penalty of $10,000 for each and every violation alleged herein.

Count XV
New York False Claims Act
N.Y. State Fin. §§ 189(1)(A)-(C) and (G)

251. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

252. This is a claim for treble damages and penalties under the New York False Claims Act.

253. By virtue of the acts described above, Defendant knowingly presented or caused

to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

254. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

255. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

256. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

257. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

258. The New York State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

259. By reason of Defendant's acts, the State of New York has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

260. Additionally, the New York State Government is entitled the maximum civil penalty of $12,000 for each and every violation alleged herein.

Count XVI
North Carolina False Claims Act
N.C. Gen. Stat. §§ 1-607(a)(1)-(3), and (7)

261. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

262. This is a claim for treble damages and penalties under the North Carolina False Claims Act.

263. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

264. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

265. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

266. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

267. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of

separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

268. The North Carolina State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

269. By reason of Defendant's acts, the State of North Carolina has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

270. Additionally, the North Carolina State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count XVII
Rhode Island False Claims Act
R.I. Gen. Laws §§ 9-1.1-3(a)(1)-(3), and (7)

271. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

272. This is a claim for treble damages and penalties under the Rhode Island False Claims Act.

273. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

274. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

275. By virtue of the acts described above, Defendants knowingly made, used, or

caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

276. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

277. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

278. The Rhode Island State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

279. By reason of Defendant's acts, the State of Rhode Island has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

280. Additionally, the Rhode Island State Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Count XVIII
Tennessee False Claims Act
Tenn. Code Ann. §§ 4-18-103(a)

281. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

282. This is a claim for treble damages and penalties under the Tennessee False Claims Act.

283. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

284. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

285. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

286. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

287. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

288. The Tennessee State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

289. By reason of Defendant's acts, the State of Tennessee has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

290. Additionally, the Tennessee State Government is entitled to the maximum penalty allowed by Tennessee law for each and every violation alleged herein.

Count XIX
Virginia Fraud Against Taxpayers Act
Va. Code Ann. §§ 8.01-216.3(a)(1)-(3), and (7)

291. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

292. This is a claim for treble damages and penalties under the Virginia Fraud Against Taxpayers Act.

293. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

294. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

295. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

296. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

297. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the State. Relator has no control over or dealings with such entities and has no access to the records in their possession.

298. The Virginia State Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

299. By reason of Defendant's acts, the State of Virginia has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

300. Additionally, the Virginia State Government is entitled to the maximum penalty of $11,000 for each and every violation alleged herein.

Count XX
District of Columbia Procurement Reform Amendment Act
D.C. Code Ann. §§ 2-308.14(a)(1)-(3), and (7)

301. Relator realleges and incorporates by reference the allegations contained in paragraphs 1 through 110 above as though fully set forth herein.

302. This is a claim for treble damages and penalties under the District of Columbia Procurement Reform Amendment Act.

303. By virtue of the acts described above, Defendant knowingly presented or caused to be presented, false or fraudulent claims for video surveillance software, hardware and related services to the State for payment or approval.

304. By virtue of the acts described above, Defendant knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for video surveillance software, hardware and related services.

305. By virtue of the acts described above, Defendants knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the State, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the State.

306. By virtue of the acts described above, Defendants have conspired, with NetDesign and others of its partners and affiliates, to commit statutory violations as set forth in the preceding three paragraphs.

307. Relator cannot at this time identify all of the false claims for payment that were caused by Defendant's conduct. The false or fraudulent claims were presented by a multitude of separate entities across the District of Columbia. Relator has no control over or dealings with such entities and has no access to the records in their possession.

308. The District of Columbia Government, unaware of the falsity of the records, statements and claims made, used, presented or caused to be made, used or presented by Defendant, paid and continues to pay the claims that would not be paid but for Defendant's unlawful conduct.

309. By reason of Defendant's acts, the District of Columbia has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

310. Additionally, the District of Columbia Government is entitled to the maximum penalty of $10,000 for each and every violation alleged herein.

Prayer

WHEREFORE, Relator prays for judgment against Defendant as follows:

1. that Defendant cease and desist from violating 31 U.S.C. § 3729 et seq., and the counterpart provisions of the State statutes set forth above;

2. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the United States has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of 31 U.S.C. § 3729;

3. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of California has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of Cal. Govt. Code § 12651(a);

4. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Delaware has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of 6 Del. C. § 1201(a);

5. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Florida has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of Fla. Stat. Ann. § 68.082(2);

6. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Hawaii has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of Haw. Rev. Stat. § 661-21(a);

7. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Illinois has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of 740 Ill. Comp. Stat. § 175/3(a);

8. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Indiana has sustained because of Defendant's actions, plus a civil penalty of $5,000 for each violation of Ind. Code Ann. § 5-11-5.5-2(b);

9. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Massachusetts has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of Mass. Gen. L. Ch. 12 § 5B;

10. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Minnesota has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of Minn. Stat. § 15C.02(a);

11. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Montana has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of Mont. Code Ann. § 17-8-401;

12. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Nevada has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of Nev. Rev. Stat. Ann. § 357.040(1);

13. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of New Hampshire has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of N.H. Rev. Stat. Ann. § 167.61-b(I).

14. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of New Jersey has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of N.J. Stat. § 2A:32C-3;

15. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of New Mexico has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of N.M. Stat. Ann. § 27-2F-4;

16. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of New York has sustained because of Defendant's actions, plus a civil penalty of $12,000 for each violation of N.Y. State Fin. § 189(1);

17. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of North Carolina has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of N.C. Gen. Stat. § 1-607(a);

18. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Rhode Island has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of R.I. Gen. Laws § 9-1.1-3(a);

19. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Tennessee has sustained because of Defendant's actions, plus the maximum civil penalty allowable for each violation of Tenn. Code Ann. §§ 4-18-103(a) and 71-5-182(a)(1);

20. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the State of Virginia has sustained because of Defendant's actions, plus a civil penalty of $11,000 for each violation of Va. Code Ann. § 8.01-216.3(a);

21. that this Court enter judgment against Defendant in an amount equal to three times the amount of damages the District of Columbia has sustained because of Defendant's actions, plus a civil penalty of $10,000 for each violation of D.C. Code Ann. § 2-308.14(a);

22. that Relator be awarded the maximum amount allowed pursuant to § 3730(d) of the False Claims Act, and the equivalent provisions of the State statutes set forth above;

23. that Relator be awarded all costs of this action, including attorneys' fees and expenses; and

24. that Relator recover such other relief as the Court deems just and proper.

Demand for Jury Trial

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Relator hereby demands a trial by jury.

Dated: May 10, 2011

By: /s/ Brian M. Melber
Brian M. Melber
bmm@personiusmelber.com
Rodney O. Personius
rop@personiusmelber.com
Personius Melber LLP
2100 Main Place Tower
Buffalo, NY 14202
Tel: (716) 855-1050
Fax: (716) 855-1052

Timothy P. McCormack
tmccormack@phillipsandcohen.com
PHILLIPS & COHEN LLP
2000 Massachusetts Ave, NW
Washington, DC 20002
Tel: (202) 833-4567
Fax: (202) 833-1815

Attorneys for Qui Tam Plaintiff James Glenn