UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DERRICK SIMS, individually, and on behalf of all others similarly situated, *Plaintiff*, v. UNITED STATES OF AMERICA, OFFICE OF PERSONNEL MANAGEMENT; and KEYPOINT GOVERNMENT SOLUTIONS *Defendants*.	C.A. No: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Derrick Sims ("Plaintiff"), individually and on behalf of all persons similarly situated (the "Class" or "Class Members"), by and through his undersigned counsel of record, brings this Class Action Complaint against Defendants, United States of America, Office of Personnel Management ("OPM") and KeyPoint Government Solutions, Inc. ("KeyPoint"), and alleges:

NATURE OF THE ACTION

1. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), Plaintiff brings this Class action lawsuit against Defendants for their failure to adequately safeguard and secure the financial and other personally identifiable information including the names, addresses, fingerprints, and social security numbers (collectively "Personally Identifiable Information" or "PII") of Plaintiff and Class Members.

2. This action stems from the unauthorized access of OPM's computer storage systems.

3. In December 2014, KeyPoint—OPM's contractor handling most federal background checks at the time—announced that its computer network had been breached ("KeyPoint Hack"). Although an OPM official maintained that there was "no conclusive evidence to confirm sensitive information was removed from the system," OPM stated its intent to notify 48,439 federal workers that their information may have been exposed.

4. In the summer of 2015, OPM confirmed multiple incursions into its own computer systems based on what OPM described as misuse of a KeyPoint user's credentials ("the OPM Breach").

5. OPM announced that the OPM Breach resulted in the pilfering of 22.1 million individuals' PII, including Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal, and financial history; and other details. Compromised records included fingerprints and findings from interviews conducted by background investigators. Usernames and passwords associated with the background investigation forms were also stolen.

6. OPM noted that the total number of individuals affected includes 19.7 million people that applied for a background investigation and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants.[1]

[1] "The vast majority of those affected — 21.5 million people — were included in an OPM repository of security clearance files, officials said. At least 4.2 million people were affected by the breach of a separate database containing personnel records including Social Security numbers, job assignments, and performance evaluations. About 3.6 million of those affected were in both systems, an overlap that accounts for the 22.1 million total, officials said." Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST, July 9, 2015, *available at*, http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

7. This massive data theft followed years of warnings, commencing in 2007 and culminating in a November 2014 audit report, from OPM's Office of Inspector General ("OIG"), which informed the agency that its computer systems contained myriad material weaknesses.

8. Despite the unequivocal notice provided by the KeyPoint Hack and the OIG's yearly admonitions, OPM elected to keep its systems operational but without fortification and without adequate security measures. OPM's inaction resulted in the successful massive cyber-attack and theft of millions of federal applicants' and related non-applicants' PII records, and other sensitive information.

9. Plaintiff, on behalf of himself and others similarly situated, alleges that through its conduct Defendants violated the Privacy Act of 1974 and the Administrative Procedure Act. Plaintiff requests damages to compensate him and Class members for current and future losses. Plaintiff also seeks injunctive relief to fix OPM's security protocol, to implement the OIG's latest audit instructions, to provide adequate credit monitoring services for a sufficient time period, to provide after-the-fact identity repair services and identity theft insurance to protect Class members from fraud or identity theft, and to re-issue certain government issued identification and documentation, such as Social Security numbers, passport numbers, and government insurance ID numbers.

PARTIES, JURISDICTION AND VENUE

10. Plaintiff Derrick Sims is an individual residing in Norwood, Massachusetts.

11. Plaintiff enlisted in the United States Marine Corps in 2007. His Military Occupation Specialty was in Aviation Ordnance. Plaintiff obtained a secret clearance in 2007, in the course of which he submitted form SF-86.

12. Defendant OPM is a United States agency with headquarters at 1900 E. Street, NW, Washington, D.C. 20415. OPM handles many aspects of the federal employee recruitment process, including managing federal job announcements, conducting background investigations and security clearances, overseeing federal merit systems, managing personal retirement and health benefits, providing training and development programs, and developing government personnel policies. As part of the recruitment and hiring process, OPM collects and maintains federal applicants' and related non-applicants' records including PII, background investigations, and security clearance forms. OPM conducts more than two million background investigations annually, provides critical human resources services to other agencies, and audits agency personnel practices.

13. Defendant KeyPoint describes itself as a "leading provider of investigative and risk mitigation services to government organizations, including the U.S. Office of Personnel Management, Customs and Border Protection and Department of Homeland Security." KeyPoint maintains its corporate headquarters in Loveland, Colorado; KeyPoint maintains its Washington, D.C., area headquarters at 8260 Willow Oaks Corporate Drive, Suite 320, Fairfax, VA 22031-4513. In recent, prepared testimony before the House Committee on Oversight and Governance Reform, KeyPoint's President and CEO described KeyPoint's work for the OPM as "provid[ing] fieldwork services for background investigations." KeyPoint employs investigators in every state, and, as of December 2014, is reported to be the largest private clearance firm working for federal agencies.

14. This Court has subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this action has been brought as a class action, the aggregate claims of the putative Class members exceed $5 million exclusive of

interest and costs, the proposed class includes in excess of 100 members, and one or more of the members of the putative Class resides in a state different from that of Defendants.

15. This Court also has subject matter jurisdiction over the federal claims in this action pursuant to 28 U.S.C. § 1331.

16. This Court also has subject matter jurisdiction over the Privacy Act of 1974 claim pursuant to 5 U.S.C. § 552a(g)(l).

17. Venue is proper in this judicial district under 28 U.S.C. §1391(b)(2) (c)(2), and (e) because, as alleged herein, a substantial portion of the events and conduct giving rise to the claim occurred in this District, Defendant KeyPoint resides in this District in that it is subject to the Court's personal jurisdiction with respect to causes of action alleged herein, and because an agency of the United States is a defendant herein and Plaintiff resides in this District.

18. Venue is also proper in this District under 5 U.S.C. § 552a(g)(5), because Plaintiff resides in this District.

19. This Court has personal jurisdiction over OPM because OPM has systematic and continuous contacts with this District and a significant amount of the relevant conduct occurred in this District.

20. This Court has personal jurisdiction over KeyPoint because it conducts significant business in this District, has systematic and continuous contacts with this District, and a significant amount of the relevant conduct from which Plaintiff's claims arise occurred in this District.

FACTUAL ALLEGATIONS

A. OPM's Responsibility for Copious Amounts of Confidential and Sensitive Personnel Data

21. OPM is an independent government agency that manages the civil service of the U.S. government. OPM handles a broad range of federal employee related issues, including managing job announcements and setting policies on government-wide hiring procedures, and conducting background investigations for prospective employees and for security clearances across the government.

22. As part of those duties, OPM collects and stores large amounts of government-wide human resources data for millions of federal employees and contractors working in all branches of government. OPM manages the electronic Official Personnel Folder ("eOPF"), a software system that provides on-demand Web-based access to personnel folders and 24/7 concurrent access to personnel information by human resources staff and employees. The eOPF file contains employee performance records, employment history, employment benefits, federal job applications (which include social security numbers and address information, among other things), résumés, school transcripts, documentation of military service, and birth certificates.

23. OPM provides investigative products and services for over 100 federal agencies. Through its Federal Investigative Services division, OPM manages and oversees a substantial portion of the federal government's employee security clearances, which involves conducting "over two million background investigations yearly with over 650,000 conducted to support initial security clearance determinations . . . more than 90% of the Government total." OPM's background investigation utility is called EPIC, an acronym based on its major components, each

of which requires aggregation and storage of a wealth of confidential federal applicant information:

- **E,** for the Electronic Questionnaires for Investigations Processing ("e-QIP") system, a "Web-based" automated software system designed to process standard investigative forms used when conducting background investigations. The e-QIP system purports to provide a "secure internet connection to electronically enter, update, and transmit [applicants'] personal investigative data over a secure Internet connection to a requesting agency."
- **P,** for the Personal Investigations Processing Systems ("PIPS"), a background investigation case management software system that handles individual investigation requests from agencies. PIPS contains the Security/Suitability Investigations Index ("SII"), a master record of background investigations conducted on government employees.
- **I,** for Imaging, which allows users to view digitalized paper case files such as surveys, questionnaires, written reports, and other images stored in the software system.
- **C,** for the Central Verification System ("CVS"), a gold mine of background investigation data. CVS contains "information on security clearances, investigations, suitability, fitness determinations, Homeland Security Presidential Directive 12 (HSPD-12) decisions,[2] PIV Cards, and polygraph data."

[2] HSPD-12 decisions are the background checks required for employees and government contractors to gain access to federal facilities.

24. Contractors and their employees who conduct security investigations for EPIC require top secret clearances.

25. CVS also contains SF-86, an extensive form that each federal applicant who is being considered for security clearance must submit. SF-86 contains vast amounts of personal data, including the security applicant's financial history and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends.

26. Prior to the OPM Breach in April 2015, OPM received a monthly average of 10 million confirmed network security intrusion attempts. Accordingly, prior to the OPM Breach, OPM was on notice of that it was heavily targeted by hackers.

B. OPM's Security Responsibilities and Failures

27. The Federal Information Security Management Act of 2002 ("FISMA")[3] was enacted to strengthen the security of information and systems within federal government agencies.

28. As part of the FISMA legislation, the Offices of Inspectors General are required to perform an independent evaluation of each agency's information security programs and practices. Under FISMA, an agency must develop, implement, and maintain a security program that assesses the risks and provides adequate security for the operations and assets of programs and software systems under its control. Specifically, FISMA requires: (1) annual agency program reviews; (2) annual Inspector General evaluations; (3) agency reporting to the Office of Management and Budget ("OMB") the results of Inspector General evaluations for unclassified

[3] At the time the OPM audits were conducted, the Federal Information Security Management Act of 2002 governed the auditing process. 44 U.S.C. §§ 3541, *et seq.* The OIG submitted the most recent audit report in November 2014. The President signed the Federal Information Security Modernization Act of 2014 into law on December 18, 2014. The Federal Information Security Modernization Act updates and supersedes the Federal Information Security Management Act. For purposes of this Complaint, "FISMA" means the Federal Information Security Management Act of 2002 and "Modernization Act" means the Federal Information Security Modernization Act of 2014.

software systems; and (4) an annual OMB report to Congress summarizing the material received from agencies. The OMB uses the reports to help it ensure that the various federal agencies are in compliance with its cyber security requirements.

29. Pursuant to FISMA, the OIG conducts yearly, independent audits of OPM's cyber security program and practices. The Department of Homeland Security ("DHS") Office of Cybersecurity and Communications issues Inspector General FISMA Reporting Instructions. Using these guidelines, the OIG reviews OPM's FISMA compliance strategy and documents the status of its compliance efforts.

30. In accordance with FISMA, the OIG must inspect the status of the following measures OPM was obliged to implement in its cyber security program: (1) Security Assessment and Authorization (the process of certifying a software system's security controls and authorizing the system for use); (2) Risk Management (risk management policies and procedures); (3) Configuration Management (controls in place to manage the technical configurations of the OPM's servers, databases, and workstations); (4) Incident Response and Reporting Programs (the procedures and requirements for reporting security incidents); (5) Security Training Program (whether employees are trained in cyber security awareness pursuant to FISMA); (6) Plans of Action and Milestones ("POA&M") Program (the use of POA&M, a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for cyber security weaknesses); (7) Remote Access Program (the policies and procedures related to authorization, monitoring, and controlling all methods of accessing the agency's network from a remote location); (8) Identity and Access Management (the policies and procedures for creating and removing user accounts, and managing user account security); (9) Continuous Monitoring Program (the efforts to continuously monitor the security state of its software systems); (10)

Contingency Planning Program (the contingency plan for potential cyber security complications); (11) Contractor Systems (the method used to maintain oversight of contractor systems); and (12) Security Capital Planning (the planning process to determine resources required to protect software systems).

31. In addition to FISMA requirements, the OIG added an additional review: the status of the OPM's Security Governance Structure—the overall framework and management structure that is the foundation of a successful cyber security program. The Security Governance Structure was designed to protect against decentralized cyber security governance, in which various departments are responsible for testing their own security. Without a single oversight team to supervise and coordinate security efforts, there is no uniformity and OPM cannot ensure that appropriate cyber security measures are in place.

32. The OIG's recent audits concluded that OPM lacked an adequate Security Governance Structure, resulting in significant non-compliance with FISMA requirements.

33. Designated Security Officers ("DSO")—officers who review software systems for cyber security weaknesses and make sure cyber security measures are in place—managed OPM's cyber security, and reported to various program offices that used software systems. The DSOs are not certified cyber security professionals, however, and perform security duties in addition to their normal, full-time job responsibilities.

34. OPM's decentralized cyber security governance structure has been in place since at least 2009. OPM attempted to centralize the DSOs in 2012 by notifying its departments that cyber security responsibilities would be overseen by the Office of the Chief Information Officer ("OCIO"). By 2014, however, OPM had only partially implemented the centralization.

35. Despite designating four centralized officers to oversee the work of the DSOs, the OIG recognized many software systems were not centralized.

36. In its 2014 audit report, the OIG noted compliance problems in a number of areas:

- Eleven major OPM systems were operating with a valid authorization;
- OPM had not fully established a Risk Executive Function;
- All operating systems were not routinely scanned for compliance with configuration baselines;
- OPM does not maintain a comprehensive inventory of servers, databases, and network devices;
- Systems were not adequately monitored;
- Program offices are not adequately incorporating known weaknesses into Plans of Action and Milestones (POA&M) and the majority of systems contain POA&Ms that were more than 120 days overdue;
- Security controls for all OPM systems were not adequately tested;
- Not all OPM systems had conducted contingency plan tests in FY 2014;
- Several information security agreements between OPM and contractor-operated information systems had expired; and
- Multi-factor authentication was not required to access OPM systems.

37. The lack of multi-factor authentication is especially noteworthy. Multi-factor authentication requires more than one form of independent credentials to verify the user's identity to access software systems, thus increasing the barriers to cyber-attack. An example is the combination of a password (something known to the user) and a Personal Identification Verification ("PIV") card (something possessed by the user). The OIG found that **none** of OPM's major applications required PIV authentication in the identification process.

38. PIV cards are identification cards used to access software systems. Data is stored on the card through an embedded smart card chip. When accessing a software system, the user

must insert the card into a card reader and provide a Personal Identification Number ("PIN"). The PIV card and PIN verifies the user's identity and allows access to the software system.

39. The November 2014 Audit Report also identified flaws in OPM's Security Assessment and Authorization: a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system, and the official management decision to authorize operation of an information system and accept its risks.

40. FISMA requires that major software systems be reassessed and reauthorized every three years, or in the alternative, continuously monitored. The OMB requires all federal software systems to have a valid authorization—a DSO must perform a comprehensive check of the cyber security of a software system to ensure that it meets all security requirements, and approve the software system for operation—and prohibits the operation of software systems without authorization. Despite these OMB requirements, the OIG found that only 10 of 21 software systems due for authorization were completed on time. The remaining systems were operating without valid authorization. The OIG found that the "drastic increase in the number of [software] systems operating without valid authorization is alarming and represents a systemic issue of inadequate planning by OPM [] to authorize the [software] systems that they own."

41. The OIG recognized that many of the unauthorized systems were "amongst the most critical and sensitive applications owned by the agency." Because two of the unauthorized systems were general support systems, and 65 percent of all software systems operated by OPM resided in those two support systems, the majority of OPM's systems were subject to any security risks that existed on the support systems.

42. Moreover, two additional systems without authorization were "owned by Federal Investigative Services, which is responsible for facilitating background investigations for

suitability and security clearance determinations." The OIG stated, "Any weaknesses in the information systems supporting this program office could potentially have national security implications."

43. Given these pandemic flaws, the OIG "recommended that OPM consider shutting down systems that do not have a current and valid Authorization."

44. OPM refused, however, and continued operating unauthorized systems.

C. OPM's History of Non-compliance

45. The 2014 Audit Report was simply the last in a long line of inspections identifying significant deficiencies in OPM's cyber security.

46. Since 2007, the OIG has "reported material weaknesses[4] in controls over the development and maintenance of the OPM's [cyber] security policies and procedures." For every year from 2009 to 2014, the OIG identified material weaknesses.

47. In 2009, the OIG first recognized a material weakness in OPM's "overall [cyber] security governance program," noting that OPM failed to fill key cyber security leadership positions.

48. In 2010, the OIG again found a "material weakness" in OPM's cyber security governance and Security Assessment and Authorization.

49. In 2011, the OIG again concluded that OPM's cyber security governance was a "material weakness," and its authorization process was inconsistent among departments.

[4] The Government Accountability Office describes a "material weakness" as a deficiency or combination of deficiencies in internal controls such that there is a reasonable possibility that a weakness in an agency's systems security program or management control structure will not "be prevented, or detected and corrected on a timely basis."

50. Cyber security governance remained a material weakness in 2012, despite the hiring of a new Chief Information Security Officer ("CISO"), because OPM did not give the CISO authority to oversee the DSOs.

51. OIG also found that when employees accessed software systems using a remote access session, the remote access would not terminate if the user failed to log off. Thus, if an employee failed to sign off, other parties could access the system from the same computer without having to enter login credentials. This security gap remained in 2014.

52. In 2013, the OIG concluded that "[l]ittle progress was made" to address the lack of "a centralized security management structure," and expressed doubt as to OPM's ability to manage major software systems. The OIG also noted that OPM failed to require PIV authentication for any of the 47 major applications.

53. In the 2014 Audit Report, the OIG found that OPM's noncompliance with FISMA was intentional and that one of the "core causes" was the "fact that there are currently no consequences for OPM systems that do not have a valid Authorization to operate."

D. OPM's Experience with System Hacks

54. Notice of its cyber security failure was also provided by a number of actual breaches leading up to the OPM Breach at issue here.

55. For example, in July 2014, the New York Times publicized an attempted intrusion in March 2014. Hackers reportedly targeted files of thousands of employees applying for security clearances; however, OPM sent an email to its employees assuring that it had not identified any loss of PII.

56. In August 2014, media sources revealed that US Investigations Services LLC ("USIS"), a contractor providing the bulk of background checks for federal security clearances—

including for OPM—had been hacked, potentially exposing thousands of government employee records. After the breach, OPM terminated its contract with USIS.

E. The KeyPoint Hack

57. In December 2014, OPM alerted more than 48,000 federal employees that their personal information may have been exposed following a data breach at KeyPoint (the "KeyPoint Hack").

58. Following USIS's termination, KeyPoint became the largest government contractor performing private employee clearances. However, because USIS's caseload was significant and involved 21,000 background checks per month, the combination of a fast transition to a new company and the rapid hiring of new employees was a perfect recipe for a break-down in the integrity of the system-access credentials, and for hackers to slip into the network during the confusion.

59. To date, KeyPoint has been unable to identify how the KeyPoint Hack occurred because KeyPoint lacked logs to track malware.

60. Following the KeyPoint Hack, the DHS and other agencies began helping OPM monitor its network.

F. The OPM Breach

61. On June 4, 2015, OPM announced it would notify approximately 4 million current and former federal applicants and employees that its software system had been hacked and employees' PII had been stolen. Though it only made the OPM Breach public on June 4, 2015, OPM detected the intrusion as early as April 2015.

62. OPM offered credit report access, 18 months of credit monitoring, and identity theft insurance and recovery services to affected current and former federal employees. In

addition, OPM issued guidance to individuals to monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.

63. U.S. investigators believe that the hackers registered several website domains with authentic sounding names such as "opmsecurity.org" and "opmlearning.org" to try and capture employee names and passwords. Because OPM did not use PIV cards or have any other multifactor authentication on its systems, the hackers were able to use the stolen credentials at will to access software systems from within and potentially even from outside the network. By using credentials to get into the software system, hackers could ferry data out of the network through the Internet, hiding its activity internally among normal traffic. It was only when OPM was assessing its software systems to actually implement continuous monitoring tools, as required by FISMA, that it discovered something was amiss.

64. The two systems breached were the eOPF system, and the central database behind "EPIC"—the software used by Federal Investigative Services in order to collect data for government employee and contractor background investigations.

65. OPM confirmed a "separate but related cybersecurity incident[]" on July 9, 2015, that affected 22.1 million individuals. The news release stated that OPM "has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. As noted above, some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints.... If an individual underwent a background investigation through OPM in 2000 or afterwards ... it is highly likely that the individual is impacted by this cyber

breach. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely."

66. OPM further confirmed that the stolen records included "identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other details. Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen."

67. After detecting the breach, OPM failed to disclose in a timely or adequate manner the facts surrounding the OPM Breach, including what happened, why it happened, who was affected, and what was stolen.

68. Rather than taking responsibility for its longstanding, documented failures, OPM has sought to shift blame for the OPM Breach to KeyPoint.

69. Former OPM Director Katherine Archuleta ("Archuleta") has stated, "[I]f anyone is to blame, it is the perpetrators." However, outside data security experts agree that the OPM Breach could have been avoided through the implementation of common security measures that were not only recommended repeatedly by the OIG, but are also mandated by federal law.

70. Moreover, Archuleta's decision not to shut down many of the critically vulnerable OPM software systems in late 2014—in contravention of the OIG's recommendation—further led directly to the OPM Breach.

G. Damage

71. In the OPM Breach, hackers stole eOPF files that contain employee performance records, employment history, employment benefits information, federal job applications, résumés, school transcripts, documentation of military service, and birth certificates. The compromised federal job applications include social security numbers, mailing addresses, birthplaces, and other names used. According to one recent report, "foreign hackers compromised the intimate personal details of an untold number of government workers. Likely included in the hackers' haul: information about workers' sexual partners, drug and alcohol abuse, debts, gambling compulsions, marital troubles, and any criminal activity." In questioning Archuleta, Senator Benjamin Sasse similarly observed "[a]s those of us who've been through top secret background checks know, they ask lots of questions about sexual history, relationships, associations, anything that could lead an individual to be coerced or blackmailed." He asked "[c]an you help us understand why this information would have been stored on OPM's networks to begin with?" Archuleta responded that OPM is still trying to "understand how that data was saved" and admitted "I actually don't know what is stored in which files."

72. In an article published in the Washington Post, Ed Mierzwinski, Federal Consumer Program Director, stated that information contained in federal job applications can be used to set up fraudulent lines of credit. Mierzwinski recommended that federal applicants tell credit monitoring agencies to stop any new lines of credit from being opened in their name. To do that, a federal applicant would be required to contact all three of the major credit monitoring agencies and pay a fee—between $10 and $15 per agency—to freeze and unfreeze each time the applicant wants to open a line of credit. Mierzwinski stated that monitoring services, like the one

OPM is providing, create a false sense of security because if data is sold off, it could take a long time before it's used.

73. In testimony before the Subcommittee on Information Policy, Census and National Archives of the Committee on Oversight and Government Reform, Daniel Bertoni, Director of the United States Government Accountability Office's ("GAO") Education, Workforce and Income Security Team, stated, "Many victims of identity theft face substantial costs and inconvenience repairing damage to their credit records . . . and some have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit [as a result of identity theft]." Bertoni stated that annually as many as 10 million people discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion.

74. The records stolen in the OPM Breach also have national security implications. The hackers accessed EPIC, and stole the SF-86 forms all service members and civilians seeking security clearance are required to fill out. The SF-86 forms require federal applicants to disclose personal information about details on alcohol and drug use, mental illness, credit ratings, bankruptcies, arrest records, and court actions. The SF-86 "gives you any kind of information that might be a threat to [the employees'] security clearance," said Jeff Neal, a former DHS official, "[i]t's really a personal document."

75. Login credentials stolen in the OPM Breach are reportedly being offered for sale on the Internet. Indeed, just one week after the OPM announced the first breach on June 4, 2015, Chris Roberts, a security expert and founder of OneWorldLabs, a company that patrols the Internet for data that could compromise clients' security, uncovered 9,500 government login credentials that were stolen from a number of government offices across the country. According

to Roberts, "[t]he recent OPM breach was identified, noted and the credentials and identities have been discovered online and are being traded actively."

76. Plaintiff and millions of other Class members have been seriously and similarly harmed by OPM's mishandling of their sensitive PII. Detailed information about all aspects of Plaintiff's and Class members' lives has been stolen and is now in the hands of criminals to be bought, sold or otherwise distributed for the purpose of misappropriating Plaintiff's identity or property. Only through aggressive and comprehensive identity theft solutions can the security of Plaintiff's and Class members' identity be maintained in the wake of the OPM Breach.

77. Plaintiff and Class members have suffered and will continue to suffer damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress. They have suffered or are at increased risk of suffering from:

- the loss of the opportunity to control how their PII is used;
- the diminution in the value and/or use of their PII, entrusted to OPM for the purpose of employment with the understanding that OPM and its employees/managers would safeguard their PII against theft and not allow access and misuse of their PII by others;
- the compromise, publication and/or theft of their PII and the PII of others, including family members, listed in the applications, including on form SF-86;
- out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to

prevent, detect, contest and recover from identity and health care/medical data misuse;

- costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;
- unauthorized use of compromised PII to open new financial and/or health care or medical accounts;
- the continued risk to their PII, and the PII of their family members, which remains in OPM's possession and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession;
- current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families;
- continued risk associated with government-issued identification, including without limitation Social Security cards, passports, naturalization numbers, military service numbers and visas.

78. The token remedy offered by OPM - credit monitoring for 18 months, plus $1 million in identity theft insurance and identity restoration services through December 7, 2016 - is woefully inadequate.

79. First, the particular credit monitoring service that is being offered to victims, CSID's "Protection Plus" package, does not provide comprehensive protection. While it offers a limited version of traditional credit monitoring, it does not offer the premium three-bureau,

modern identity service, which is necessary in this instance due to the breadth of the information compromised in the OPM Breach.

80. Even so, traditional credit monitoring, when at its best, is only effective for a relatively small portion of the identity and reputational crimes these particular victims can be subjected to, due to the expansive data involved in the breach. A three-bureau report will generally catch new credit account fraud in traditional areas; however criminals can still actively sell the victims' data to underworld sites for tax identity theft, medical identity theft, and other difficult to detect forms of identity crime such as a synthetic identity theft,[5] identity theft of medical information or insurance information, or theft of professional credentials. Any credit monitoring service offered to victims of this extensive breach needs to offer more, not less protection. For all these reasons, credit monitoring alone is insufficient to repair the damage done by the OPM Breach.

81. Second, the proposed remedies do nothing to address the significant risk of reputational harm victims are exposed to in online media. Modern remediation of severe breaches includes monitoring for reputational mentions across tens of thousands of social media and other web sites to ensure breach victims are not being impersonated in social media and elsewhere online. This is an important safety precaution for those individuals who have had their information breached, particularly those with high security clearances or who work in sensitive positions.

82. Third, the proposed CSID remedy does not appear to include monitoring for criminal data sales on the dark web sites and data broker sites that deal in stolen data. This is a

[5] Synthetic identity theft involves the use of verifiable information stolen from one or more victims to create a fictitious identity that will be verifiable because the individual elements are legitimate.

necessary service that is offered for victims of identity theft and data breaches, particularly where the data stolen is as sensitive as it was in the OPM Breach. As discussed above, evidence suggests that this information already has been, and continues to be, bought and sold on the black market.

83. Finally, the 18-month duration of services currently offered by OPM is far too short. It is well documented by law enforcement professionals and identity theft experts that hackers "season" data by allowing it to age for five years or more. The more sensitive and potentially valuable the data is, the more it can be seasoned by criminals. Highly sensitive investigative background check data, which is inclusive of unique and often non-changeable data such as permanent medical conditions and the full battery of information about relatives, warrants an extended and in some cases lifetime of protection due to the completeness of the data and its high value on the black market.

CLASS ACTION ALLEGATIONS

84. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of a class of similarly situated persons, which he initially proposes be defined as follows:

All persons whose PII was compromised as a result of the data breaches announced by OPM on June 4, 2015 and July 9, 2015.

85. Excluded from the proposed class are OPM and KeyPoint, as well as agents, officers and directors (and their immediate families) of OPM and KeyPoint, their parents, subsidiaries, affiliates and controlled persons. Also excluded is any judicial officer assigned to this case.

86. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4).

87. Numerosity—Fed. R. Civ. P. 23(a)(1). The members of the class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiff at the present time and can only be ascertained through appropriate discovery, Plaintiff believes that there are 21 million or more members of the class located throughout the United States. It would be impracticable to join the class members individually.

88. Existence and predominance of common questions of law—Fed. R. Civ. P. 23(a)(2), 23(b)(3). Common questions of law and fact exist as to all members of the class and predominate over any questions solely affecting individual members of the class.

89. Among the many questions of law and fact common to the class are:

- whether OPM's conduct violated the Privacy Act of 1974;
- whether OPM failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records;
- whether OPM disclosed Plaintiff's and Class members' PII without their prior written consent;
- whether Defendants' conduct was willful or with flagrant disregard for the security of Plaintiff's and Class Members' PII;
- whether Defendants had a legal duty to use reasonable cyber security measures to protect Plaintiff's and Class members' PII;

- whether Defendants breached their legal duty by failing to protect Plaintiff's and Class members' PII;
- whether Defendants acted willfully in failing to secure Plaintiff's and Class members' PII;
- whether Plaintiff and Class members are entitled to damages, declaratory or injunctive relief.

90. Typicality—Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of the members of the class. Among other things, Plaintiff and Class members are federal applicants, non-applicants related to or associated with federal applicants, and former, current, and prospective employees and contractors of the federal government who filed SF-86 and other sensitive documentation with OPM.

91. Adequacy—Fed. R. Civ. P. 23(a)(4). Plaintiff will adequately represent the proposed Class members. He has retained counsel competent and experienced in class action and Internet privacy litigation and intend to pursue this action vigorously. Plaintiff has no interests contrary to or in conflict with the interests of class members.

92. Superiority—Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

93. In the alternative, the class may be certified under Rule 23(b)(1), 23(b)(2) or 23(c)(4) because:

- the prosecution of separate actions by the individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants;
- the prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;
- Defendants acted or refused to act on grounds generally applicable to the class, thereby making appropriate final injunctive relief with respect to the members of the class as a whole; and
- the claims of class members are comprised of common issues that are appropriate for certification under Rule 23(c)(4).

CAUSES OF ACTION

COUNT ONE
(On behalf of Plaintiff and Class Members against OPM)

VIOLATION OF PRIVACY ACT OF 1974, 5 U.S.C. § 552a ("PRIVACY ACT")

94. Plaintiff incorporates the previous allegations as if fully set forth herein.

95. OPM is an "agency" within the meaning of the Privacy Act.

96. Pursuant to 5 U.S.C. § 552a(b), agencies are prohibited from disclosing "any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."

97. Pursuant to 5 U.S.C. § 552a(e)(10), "[e]ach agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

98. OPM obtained and preserved the PII of Plaintiff and Class members in a system of records during the recruiting and security check processes.

99. OPM is therefore prohibited from disclosing Plaintiff's and Class members' PII and is responsible for establishing appropriate "safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity" under 5 U.S.C. § 552a(e)(10).

100. OPM is, and at all relevant times was, required by law to comply with both FISMA and the Modernization Act. OPM is also responsible for ensuring that its cyber security systems comply with 5 U.S.C. § 552a and other rules and regulations governing cyber security practices.

101. However, as alleged herein, OPM intentionally and willfully failed to comply with FISMA and the Modernization Act and 5 U.S.C. § 552a and other rules and regulations governing cyber security practices.

102. OPM knew that its computer security practices were not in compliance with 5 U.S.C. § 552a, FISMA, the Modernization Act, and other rules and regulations governing cyber security practices because the OIG's annual audit reports have consistently recognized OPM's noncompliance with FISMA.

103. Through a continuous course of conduct, OPM thus willfully and intentionally refused to take steps to implement "appropriate safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity."

104. OPM's history of non-compliance with FISMA's legal requirements that culminated in OPM's decision not to follow the OIG's 2014 recommendation to shut down information systems that did not have current and valid authorizations resulted in (1) the disclosure of Plaintiff's and Class members' records without prior written consent in violation of 5 U.S.C. § 552a(b) and ultimately (2) the "substantial harm, embarrassment, inconvenience, or unfairness" to Plaintiff and Class members, that 5 U.S.C § 552a(e)(10) is designed to protect against.

105. As a result of OPM's conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the Privacy Act. Such damages have included or may include without limitation (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to OPM for the purpose of deriving employment from OPM and with the understanding that OPM and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to prevent, detect, contest and

recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets, and re-issuance fees for visas or other compromised credentials; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) the continued risk to their PII, and the PII of their family members, neighbors, and acquaintances, which remains in OPM's possession and is subject to further breaches so long as OPM fails to undertake appropriate and adequate measures to protect the PII in its possession; (9) the continued risk associated with government-issued identification, including without limitation Social Security cards, passports, naturalization numbers, and military service numbers and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families. Plaintiff and Class members are thus entitled to relief pursuant to 5 U.S.C. §§ 552a(g)(l)(D) and (g)(4).

COUNT TWO
(On behalf of Plaintiff and Class members against OPM)

VIOLATION OF THE ADMINISTRATIVE PROCEDURE ACT,
5 U.S.C. §§ 701, *et seq.*

106. Plaintiff incorporates the previous allegations as if fully set forth herein.

107. OPM was required to comply with FISMA and has a continuing obligation to comply with the Modernization Act. Moreover, under FISMA, Archuleta was required to exercise oversight over OPM's information security policies and practices, including implementation of rules and standards complying with 40 U.S.C. § 11331. However, as is alleged herein, from 2009 to 2014, through a continuous course of conduct, OPM intentionally failed to

comply with FISMA and 40 U.S.C. § 11331 resulting in violations of the Privacy Act, 5 U.S.C. § 552a.

108. OPM's non-compliance with FISMA's requirements was consistent from 2009 to 2014 and was not a valid exercise of discretion. FISMA and the Modernization Act are the law and pursuant to FISMA's terms, Archuleta was required to oversee OPM's compliance with both. The OIG found that she failed to do so and that her failure was caused in large part by the absence of any consequence for such noncompliance. Ultimately OPM's noncompliance with FISMA and the Modernization Act resulted in the Privacy Act violations at the center of this lawsuit.

109. OPM's noncompliance with FISMA is well documented in each of the OIG's annual audit reports issued from 2009 to 2014. As alleged above, in each of the OIG's audit reports, the OIG instructed OPM to bring its cyber security systems in compliance with FISMA, but each year, OPM made the decision not to do so. For example, from 2011 to 2014, the OIG told the OPM it was not in compliance with FISMA because of its decentralized cyber security governance system. Yet OPM repeatedly made the decision not to comply with FISMA's requirements. And in 2014, the OIG specified: "OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

110. OPM's continual failure to comply with FISMA culminated in Archuleta's choice not to follow the OIG's November 2014 recommendation to shut down several of its compromised software systems. In the 2014 audit report, the OIG found 11 of 21 software systems were unauthorized, meaning that those software systems had not been checked to determine whether they were vulnerable to a data breach. The OIG recommended that OPM shut down "[software] systems that do not have a current and valid authorization." However, OPM refused to shut down its software systems. At the Committee Hearing, Archuleta stated, "It was

my decision that we would not [close down the software systems] but continue to develop the systems and ensure we have security on those systems."

111. OPM's many decisions not to comply with FISMA and OMB requirements including, but not limited to, (1) deciding not to implement a centralized cyber security governance system, (2) deciding not to use PIV authentication for all of their systems, and (3) deciding not to follow the OIG's recommendation and shut down its software systems, constitute final agency actions because the decisions were the consummation of OPM's decision making process, were not of a merely tentative or interlocutory nature, and denied Plaintiff and Class members the right to protection of their PII. Because OPM's willful and intentional continuous course of conduct resulted in the OPM Breach in which Plaintiff's and Class members' PII was compromised, OPM's continuous string of decisions not to comply with FISMA caused violations of the Privacy Act and damages to Plaintiff and Class members.

112. OPM violated its obligation to comply with FISMA, 40 U.S.C. § 11331, and the Privacy Act because, for years, OPM ignored the OIG's detailed instructions and ultimately, decided to reject its instruction that OPM shut down certain of its major software systems that were not in compliance with FISMA.

113. OPM's continuous string of decisions not to comply with FISMA—including its decisions not to implement a centralized cyber security governance system and its refusal to shut down OPM's software systems in contravention of the OIG's instructions—was arbitrary, capricious and otherwise not in accordance with law; was in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; and was without observance of procedure required by law.

114. Because of OPM's decisions not to comply with FISMA, OPM violated the Privacy Act, Plaintiff and Class members suffered a legal wrong, and were adversely affected insofar as cyber attackers gained access to their sensitive, confidential, and personal information.

115. Absent a claim under the Administrative Procedure Act, Plaintiff does not have an adequate remedy at law to seek injunctive and declaratory relief against OPM.

116. Plaintiff and Class members are thus entitled to declaratory and injunctive relief.

COUNT III
(On behalf of Plaintiff and Class members against KeyPoint)

NEGLIGENCE

117. Plaintiff incorporates the previous allegations as if fully set forth herein.

118. From 2014 to present, KeyPoint has worked as a contractor for OPM responsible for conducting background checks on federal applicants. KeyPoint's employees were granted access to OPM's systems containing Plaintiff's and Class members' PII.

119. KeyPoint owed Plaintiff and Class members a duty to take reasonable steps to maintain and protect against any dangers to Plaintiff's and Class members' PII presented by cyber attackers. This duty included, among other things, maintaining and testing KeyPoint's cyber security systems, taking other reasonable security measures to protect and adequately secure the PII of Plaintiff and Class members from unauthorized access, and taking reasonable steps to ensure that hackers did not compromise KeyPoint employees' credentials.

120. KeyPoint owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate cyber security practices. It was foreseeable that if KeyPoint did not take reasonable security measures—including protecting its OPM credentials—the PII of Plaintiff and Class members could be stolen. KeyPoint knew or should

have known that OPM employee data was an attractive target for cyber attackers, particularly in light of the prior data breaches experienced by OPM and its contractors, and yet KeyPoint failed to take reasonable precautions to safeguard the PII of federal applicants and related non-applicants.

121. In December 2014, OPM announced that KeyPoint's cyber security systems sustained a breach. In that breach, cyber attackers were able to access KeyPoint's OPM credentials, which, according to Archuleta, facilitated the massive OPM Breach that compromised the PII of approximately 22 million individuals.

122. By failing to implement necessary measures to protect KeyPoint's security credentials, KeyPoint departed from the reasonable standard of care and breached its duties to Plaintiff and Class members.

123. But for KeyPoint's failure to implement and maintain adequate security measures to protect Plaintif's and Class members' PII, and failure to adequately log security intrusions into its software systems, the PII of Plaintiff and Class members would not have been stolen, Plaintiff and Class members would not have been injured, and Plaintiff and Class members would not be at a heightened risk of identity theft in the future.

124. KeyPoint's negligence was a substantial factor in causing harm to Plaintiff and Class members. As a direct and proximate result of KeyPoint's failure to exercise reasonable care and deploy reasonable cyber security measures, the PII of Plaintiff and Class members was accessed by cyber attackers who can use the compromised PII to commit identity theft and any variety of serious fraud.

125. As a result of KeyPoint's negligence, Plaintiff and Class members have suffered damages that have included or may include without limitation: (1) the loss of the opportunity to

control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to OPM and KeyPoint for the purpose of deriving employment from OPM and with the understanding that OPM and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the OPM Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) the continued risk to their PII, and the PII of their family members, neighbors, and acquaintances, which remains in KeyPoint and OPM's possession and is subject to further breaches so long as KeyPoint and OPM fail to undertake appropriate and adequate measures to protect the PII in its possession; and (9) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the OPM Breach for the remainder of the lives of the Class members and their families.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

(a) Certify this case as a class action, appoint Plaintiff as class representative, and appoint Plaintiff's counsel to represent the class;

(b) Award Plaintiff and Class members appropriate relief, including actual and statutory damages;

(c) Award equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction requiring the U.S. government to re-issue free of charge any government-issued identification compromised by the OPM Breach, such as Social Security cards, passports, naturalization numbers, military service numbers and visas;

(d) Find that KeyPoint breached its duty to implement reasonable security measures to safeguard and protect the PII of Plaintiff and Class members that was compromised in the OPM Breach;

(e) Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

(f) Award pre-judgment and post-judgment interest as prescribed by law; and,

(g) Grant further and additional relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: September 23, 2015

Respectfully submitted,

PASTOR LAW OFFICE, LLP

/s/ David Pastor
David Pastor (BBO # 391000)
63 Atlantic Avenue, 3d Floor
Boston, Massachusetts 02110
Telephone: 617-742-9700
dpastor@pastorlawoffice.com

LEONARD LAW OFFICE, PC

/s/ Preston W. Leonard
Preston W. Leonard (BBO #680991)
63 Atlantic Avenue, 3d Floor
Boston, Massachusetts 02110
Telephone: 617-329-1295
pleonard@theleonardlawoffice.com

Attorneys for Plaintiffs and Putative Class