UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

EDWARD W. KRIPPENDORF, on behalf of himself and all others similarly situated, Plaintiff, vs. UNITED STATES OF AMERICA, OFFICE OF PERSONNEL MANAGEMENT; and KEYPOINT GOVERNMENT SOLUTIONS, Defendants.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Edward W. Krippendorf, individually and on behalf of the proposed class described below, brings this action for injunctive relief, and actual and statutory damages against Defendants the United States of America, Office of Personnel Management ("the OPM") and KeyPoint Government Solutions ("KeyPoint") and allege as follows:

I. SUMMARY OF THE CASE

1. This case arises out of multiple cyber-breaches of OPM's systems that compromised the security of more than 20 million individuals (breaches collectively referred to herein as the "OPM Breach"). The OPM Breach has been described by Congressional representatives as "the most devastating cyber attack in our nation's history." Plaintiff and Class members include current, former, and prospective employees and contractors of the U.S. government ("federal applicants"), as well as family members or other contacts of federal applicants, including spouses and co-habitants, who never applied for a position with the U.S. government, but that nonetheless had their personally identifying information ("PII") and records

compromised ("related non-applicants") because their information was provided to the U.S. government by the federal applicants as part of the application process.

2. The OPM is a government agency responsible for maintaining large amounts of data about federal applicants and related non-applicants. The OPM provides investigative services for more than 100 Federal agencies in connection with security clearance determinations and hiring decisions to ensure compliance with Executive Orders and other rules and regulations. The OPM conducts over 90% of the Government's background investigations – more than two million investigations every year.

3. As part of the OPM's security clearance protocol, applicants applying for security clearance ("security applicants") must submit detailed personal information that can include their financial histories 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 and coworkers.

4. Since at least 2007, the OPM has been on notice of significant deficiencies in its cyber security protocol. Despite the fact that the OPM handles massive amounts of private, sensitive, and confidential information of federal applicants and related non-applicants, the OPM failed to take steps to remedy those deficiencies. The OPM's Office of Inspector General ("OIG") was required under federal law to, and did, conduct annual audits of the OPM's cyber security program and practices, identifying "material weakness[es]"[1] as far back as 2007. The OPM not only failed to cure the weaknesses, but during the ensuing seven years, the OIG found

[1] 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."

that in many areas the OPM's performance actually got worse. According to a 2014 OIG report, 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 program offices to authorize the [software] systems they own." Indeed, approximately ***65% of all OPM data*** was stored on uncertified systems.

5. From 2007 to the present, the OPM repeatedly failed to comply with federal law and make the changes set forth in the OIG's annual audit reports. Thus the OPM failed to comply with the Privacy Act which requires federal agencies to safeguard systems of records by "establish[ing] 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."

6. In its November 2014 audit report, the OIG identified multiple cyber security deficiencies by the OPM that "could potentially have national security implications." These included: (1) the OPM's decentralized governance structure; (2) a lack of acceptable risk management policies and procedures; (3) failure to maintain a mature vulnerability scanning program to find and track the status of security weaknesses in software systems; (4) a high rate of false security alerts that could delay the identification of and response to actual security breaches; (5) failure to use tools to monitor the progress of corrective efforts for cyber security weaknesses; (6) remote access sessions which did not terminate or lock out after the period of inactivity required by federal law; (7) failure to continuously monitor the security controls of all software systems; (8) failure to maintain and test contingency plans for every information system as required under the OPM's policies; and (9) failure to use Personal Identification Verification

("PIV") Cards[2] for multi-factor authentication in all major software systems. As a result, the OIG concluded that the OPM's software systems were so vulnerable that the OPM should consider largely "shutting [them] down."

7. In December 2014, KeyPoint, the private OPM contractor that handled the majority of federal background checks at the time, announced that it had suffered a computer network breach. At the time, OPM spokeswoman Nathaly Arriola said that there was "no conclusive evidence to confirm sensitive information was removed from the system" but that the OPM would notify 48,439 federal workers that their information *may* have been exposed. After the OPM Breach became public the OPM identified the misuse of a KeyPoint user credential as the source of the breach.

8. Despite (1) knowledge of the recent KeyPoint breach and, (2) being explicitly warned about deficiencies in cyber security protocol and the dangers associated with those deficiencies, the OPM elected not to shut down the OPM's software systems. Subsequently, the OPM announced that it had been the subject of a massive cyber attack that compromised millions of federal applicants' and related non-applicants' PII records, and other sensitive information.

9. The combination of KeyPoint's cyber security weaknesses and the OPM's cyber security failures caused the massive scope of the OPM Breach. According to CNN, "Some investigators believe that after [the KeyPoint intrusion] last year, OPM officials should have

---

[2] PIV cards are government 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.

blocked all access from KeyPoint, and that doing so could have prevented more serious damage."

10. On June 4, 2015, the OPM issued a news release confirming that the PII of approximately 4 million current, former, and prospective Federal employees and contractors "may have been compromised."

11. After the OPM's first announcement that it had been hacked, top OPM officials were criticized by members of the House Oversight and Government Reform Committee as "grossly negligent." U.S. Representative Jason Chaffetz— chairman of the House Oversight and Government Reform Committee—likened the OPM's lax cyber security protocol to "leaving all the doors and windows open in your house and expecting that nobody would walk in and nobody would take any information." Congressman Steve Russell similarly concluded that "this is absolute negligence that puts the lives of Americans at risk . . . ."

12. On July 9, 2015, the OPM issued a second news release confirming that a significantly greater number of individuals were affected by a "separate but related" cyber security breach. The OPM announced that 22.1 million individuals had records stolen that 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."

13. The OPM confirmed that 19.7 million of those affected were federal applicants who applied for a background investigation, and another 1.8 million were non-applicants,

including family members, spouses, co-habitants and other close contacts of federal applicants, who never applied for a position with the U.S. government. In addition, approximately 1.1 million of the stolen records included fingerprints.

14. As a result of Defendants' conduct, Plaintiff and Class members have suffered and will continue to suffer actual damages and pecuniary losses, including costs associated with mitigating the risk of identity theft, such as costs for effective credit monitoring services[3] and identity theft insurance, and fees and other costs associated with re-issuing credentials.

15. Defendants' conduct violated the Privacy Act of 1974 ("Privacy Act"), the Administrative Procedure Act, and constitutes negligence.[4] Plaintiff requests damages to compensate him and Class members for current and future losses and injunctive relief to fix the OPM's security protocol, 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.

---

[3] The credit monitoring services being made available by the OPM provide only small amounts of necessary protection to Class members. They are ineffective and insufficient in protecting them from the criminals who have obtained their data through Defendants' wrongful conduct.

[4] Plaintiff, on behalf of himself and the Class, asserts negligence claims against KeyPoint in this Complaint. Plaintiff has also simultaneously filed or will shortly file an administrative claim under the Federal Tort Claims Act with OPM on behalf of himself and the Class alleging it was negligent in causing the Data Breach. Such claims are asserted in the alternative, and Plaintiff is not seeking a double-recovery for himself or the Class. Rather, Plaintiff intends to amend this Complaint to assert claims under the Federal Tort Claims Act in the event that the OPM either denies his claim or takes no action within 6 months from the submission of that claim.

II. PARTIES

A. PLAINTIFF

16. Plaintiff Edward W. Krippendorf is a resident of the Commonwealth of Massachusetts. Plaintiff Krippendorf has worked for the federal government from 1997 to 2012, first as an employee of two government contractors, Innolog and SysTeam, working on computer systems for the Department of Defense ("DOD") starting in 1997, and then working directly for the DOD as a civilian on its computer systems from December 2005 to February 2012. Plaintiff Krippendorf has received a letter from the OPM indicating that his personnel records have been compromised by the OPM Breach. Plaintiff Krippendorf also had federal security clearance from 1997 to 2012, and based on the OPM's public statements regarding the scope of the OPM Breach, Plaintiff Krippendorf's PII, records, and sensitive information were likely also compromised as a result of the OPM Breach.

B. DEFENDANTS

17. Defendant OPM is a U.S. agency with headquarters at 1900 E. Street, NW, Washington, D.C. 20415. The 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 process, the OPM collects and maintains federal applicants' and related non-applicants' records including PII, background investigations, and security clearance forms. The OPM conducts more than two million background investigations annually, provides critical human resources services to other agencies, and audits agency personnel practices.

18. 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 and 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, it was reported that KeyPoint was the largest private clearance firm working for federal agencies.

III. JURISDICTION AND VENUE

19. 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 lawsuit 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 is a resident of a different state than Defendants.

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

21. This Court also has subject matter jurisdiction over the Privacy Act of 1974 claim pursuant to 5 U.S.C. § 552a(g)(1).

22. This Court has personal jurisdiction over the OPM because it maintains headquarters in the District of Columbia and much of the relevant conduct occurred in the District of Columbia.

23. This Court has personal jurisdiction over KeyPoint because it conducts significant business in the District of Columbia and much of the relevant conduct occurred in the District of Columbia.

24. Venue is proper in this District under 28 U.S.C. § 1391 because the OPM is headquartered in this District and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District.

25. Venue is also proper in this District under 5 U.S.C. § 552a(g)(5) and 5 U.S.C. § 703.

IV. FACTUAL ALLEGATIONS

A. The Office of Personnel Management is Responsible for the Collection and Storage of a Substantial Amount of Confidential and Sensitive Personnel Records

26. The OPM is an independent government agency that manages the civil service of the U.S. government. The OPM handles a broad range of federal employee related issues including: (1) managing job announcement postings and setting policies on government-wide hiring procedures; (2) conducting background investigations for prospective employees and security clearances across the government; (3) upholding and defending the merit system in the federal civil service; (4) managing pension benefits for retired federal employees and their families and administering health and other insurance programs for federal employees and retirees; (5) providing training and development programs and other management tools for federal employees and agencies; and, (6) taking the lead in developing, testing and implementing government-wide policies relating to personnel issues.

27. The 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. The 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), resumes, school transcripts, documentation of military service, and birth certificates.

28. The OPM provides investigative products and services for over 100 federal agencies. Through its Federal Investigative Services division, the 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." The background investigation toolset is called EPIC which is 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"), the "mother lode" of background investigation data. CVS contains "information on security clearances, investigations, suitability, fitness determinations Homeland Security Presidential Directive 12 (HSPD-12) decisions,[5] PIV Cards, and polygraph data."

29. Some aspects of EPIC contain information that is so sensitive it is housed at Fort Meade—the home of Defense Information Systems Agency and National Security Agency ("NSA"). Contractors and their employees who conduct security investigations for EPIC require top secret clearances.

30. CVS additionally contains SF-86, a 127-page form that each federal applicant who is being considered for security clearance must submit. SF-86 contains huge treasure troves of personal data, including security applicants' financial histories 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 such as college roommates and coworkers. Employees log in using their Social Security numbers.

---

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

31. Leading up to the initial OPM breach in April 2015, the OPM received 10 million confirmed intrusion attempts targeting its network in an average month. As a result, the OPM was on notice of the fact that it was heavily targeted by hackers prior to the OPM Breach.

B. The OPM'S Systemic Cyber Security Failures

32. The Federal Information Security Management Act ("FISMA")[6] governs software system requirements for software systems owned or operated by federal agencies and contractors. Under FISMA, the OPM and its Director are required to "develop and oversee[] the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40."

33. 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 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.

---

[6] 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.

34. In accordance with FISMA, the OIG conducts annual, independent audits of the 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 the OPM's FISMA compliance strategy and documents the status of its compliance efforts.

35. Pursuant to FISMA, the OIG is required to review the status of the following measures the OPM was supposed to have implemented 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).

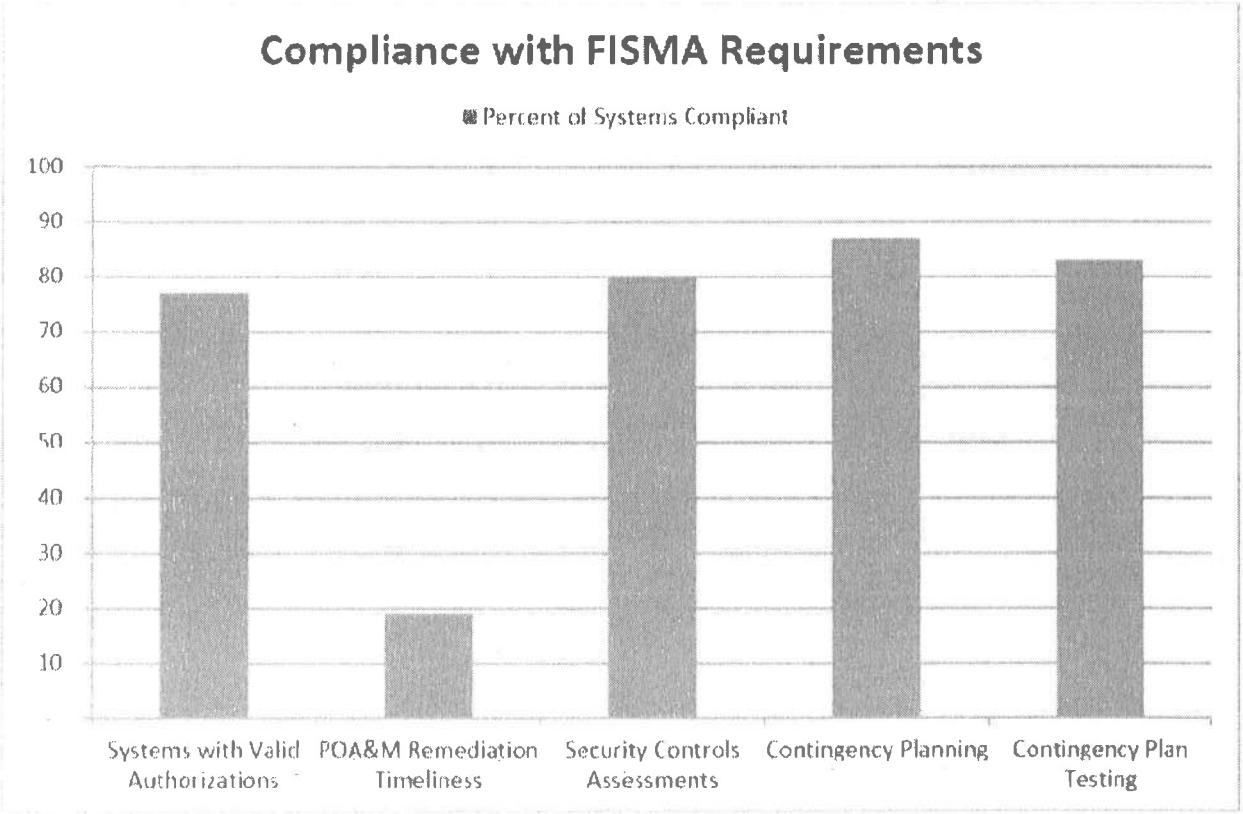
36. In addition to FISMA requirements, the OIG reviews the status of the OPM's Security Governance Structure—the overall framework and management structure that is the foundation of a successful cyber security program. The OIG added this category after repeatedly recognizing problems in the OPM's governance structure over the cyber security process. The Security Governance Structure was designed to protect against decentralized cyber security governance, where various departments are responsible for testing their own security. Without one team to oversee and coordinate security efforts, there is no uniformity and the OPM cannot ensure that appropriate cyber security measures are in place.

37. Several of the OIG's recent audits concluded that the OPM lacked a centralized cyber security team responsible for overseeing all of the OPM's cyber security efforts, creating many instances of non-compliance with FISMA requirements. Designated Security Officers (DSO)—officers who review software systems for cyber security weaknesses and make sure cyber security measures are in place—managed the 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.

38. The OPM has had a decentralized cyber security governance structure since at least 2009. In 2012, the OPM attempted to centralize the DSO program by notifying its departments that cyber security responsibilities would be overseen by the Office of the Chief Information Officer ("OCIO"). However, by 2014, the OPM only partially implemented the

centralization. Although the OPM designated four centralized officers to oversee DSO's work, the OIG recognized many software systems that were not centralized.

39. As of 2014, because of the OPM's lack of a centralized cyber security governance structure, as demonstrated by the following graph from the OIG's November 2014 report, a large portion of the OPM's software systems were not in compliance with FISMA requirements.



40. Specifically, in its 2014 audit report, which covered the cyber security protocol the OPM had in place as of November 2014, the OIG noted compliance problems in a number of areas:

- The OPM lacked acceptable risk management policies and procedures, and specifically failed to assess risk, maintain a risk registry, or communicate agency-wide risks to its departments.
- The OPM failed to have appropriate configuration controls in place, specifically lacking a "mature vulnerability scanning program" to find and track the status of security weaknesses in its software systems.

- The OPM's automated security alert system reported a high rate of false security alerts that could delay the identification and response to actual security breaches. The OPM failed to effectively use POA&M. Accordingly, the OPM could not effectively identify and monitor the progress of the corrective efforts and ensure that those weaknesses were fixed.

- The OIG found that where employees accessed the OPM's system from a remote location, the remote access sessions did not terminate or lock out after the period of inactivity required by FISMA.

- The OPM failed to continuously monitor the security controls of all of its software systems, finding that only 37 of 47 software systems were adequately tested for security issues in 2014, and that it had been "over eight years since all [software] systems were subject to an adequate security controls test." The OIG noted that a "failure to continuously monitor and assess security controls increases the risk that agency officials are unable to make informed judgments to mitigate risks to an acceptable level."

- The OPM failed to maintain and test contingency plans for every software system as required under the OPM's policies. The OPM only maintained contingency plans for 41 of 47 software systems, and only tested 39 of 47 software systems.

41. In addition, the OIG found that the OPM was not in compliance with the OMB's requirements,[7] which mandate the use of PIV Cards for multi-factor authentication in all major software systems.

42. 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 of multi-factor authentication would be the combination of a password (something known to the user) and the PIV card (something possessed by the user). The OIG found that **none** of the OPM's major applications required PIV authentication in the identification process.

---

[7] The February 3, 2011 OMB Memorandum M-11-11 incorporates the DHS PIV card standards requiring all new systems to be enabled to use PIV cards prior to being made operational. Effective as of 2012, existing physical and logical access control systems must be upgraded to use PIV credentials and Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.

43. PIV cards contain computerized chips which build in an extra layer of security to ensure that only authorized users have access to secure software systems.

44. Also in its November 2014 audit report, the OIG found that a critical flaw was the OPM's Security Assessment and Authorization—its process of certifying a software system's security controls. Under FISMA, major software systems are required to 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 do a comprehensive check on the cyber security of a software system to make sure 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 rest were currently operating without valid authorization, meaning that those software systems had not been checked to determine whether they were vulnerable to a data breach. The OIG noted 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 [the] OPM [] to authorize the [software] systems they own."

45. The OIG noted that several of the unauthorized software systems were "amongst the most critical and sensitive applications owned by the agency." It warned that over 65 percent of all software systems operated by the OPM reside in two of the major support systems lacking authorization, and therefore are subject to any security risks that exist on the support systems. According to the OIG audit, 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 that "[a]ny weaknesses in the

information systems supporting this program office could potentially have national security implications."

46. The OIG also found that the OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331 ("Responsibilities for Federal Information Systems Standards"), as is required by FISMA, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, contractor systems, security capital planning, and contingency planning.

47. Because of the significant flaws in the OPM's cyber security systems, the OIG instructed that the "OPM consider shutting down systems that do not have a current and valid Authorization." The OPM refused, however, to follow this recommendation and continued to operate all of the unauthorized systems.

C. Key Vulnerabilities in the OPM's Cyber Security Protocol

48. Michael Esser, the assistant inspector general at the OIG, is responsible for auditing the security systems at the OPM. In recent prepared testimony before the House Committee on Oversight & Government Reform, Esser summarized the annual OIG audit reports, stating that the "OPM's long history of systemic failures to properly manage its IT infrastructure, which we believe ultimately led to the breaches we are discussing today." Esser highlighted three significant issues identified in the 2014 Audit.

49. **Systems Authorization.** Esser stated that the OPM has a long history of issues related to software system authorization – a critical requirement of FISMA to ensure data security. In 2010, the OIG recognized that the OPM suffered from poor management over the authorization process, OPM divisions often failed to complete authorization on software systems, and OPM failed to establish standardized authorization requirements to ensure that its divisions were not authorizing software systems with significant cyber security risks. The authorization

problem initially improved but resurfaced in 2014. Esser stated that only 10 of 21 software systems due for authorization were completed on time. The 11 software systems that were not in compliance were located in various departments including the Offices of the Chief Information Officer; Federal Investigative Services; Human Resources Solutions; Office of the Inspector General; and, Office of the Chief Financial Officer. Esser stated that it was a "drastic increase from prior years, and represents a systemic issue of inadequate planning by the OPM program offices to assess and authorize the [software] systems that they own. He went on to confirm that "[i]t already appears that there will be a greater number of [software] systems this year operating without a valid authorization," due to the OPM "temporarily put[ting] Authorization efforts on hold while it modernizes the OPM's IT infrastructure in response to security breaches." And he noted that "[a]uthorization should continue, as the modernization is likely to be a long-term effort." Esser also confirmed that in his 2014 report to the OPM, he recommended it to shut down some of its networks because they were vulnerable, which the OPM refused to do.

50. **Policies, Procedures & Technical Controls.** Esser said that two of the most critical areas in which the OPM needs to improve its technical security controls "relate to policies, procedures, and technical controls used to ensure that PIV credentials are securely deployed." He noted that the OPM has "implemented a variety of new controls and tools designed to strengthen the agency's technical infrastructure," but failed to utilize the tools to their fullest potential. He also stated that the OPM does not maintain an accurate centralized inventory of all servers and databases in its network, and that "without a comprehensive list of assets that need to be protected and monitored" the OPM cannot fully defend its network. He confirmed that the OPM failed to use PIV authentication for all 47 of the agency's major applications, adding that "[f]ull implementation of PIV authentication would go a long way in

protecting an agency from security breaches, as a [hacker] would need to compromise more than a username and password to gain unauthorized access to a system."

51. **Decentralized Cyber Security Governance.** Esser stated that for several years the OPM had been unclear which cyber security responsibilities fall on the central office, and which are left to individual departments within the OPM. In addition, he noted that some cyber security responsibilities that were left to individual departments ended up being implemented by unqualified officials: "[t]he program office personnel responsible for [cyber] security frequently had no [cyber] security background and were performing this function in addition to another full-time role." He stated that, "as a result of this decentralized governance structure, many security controls went unimplemented and/or remained untested, and the OPM routinely failed a variety of FISMA metrics year after year."

D. The OPM has Repeatedly Failed to Comply with FISMA's Cyber Security Requirements

52. The OIG's 2014 audit report followed years of recognized deficiencies in the OPM's cyber security. Since 2007, the OIG has "reported material weaknesses 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.

53. In 2009, the OIG first recognized a material weakness in the OPM's "overall [cyber] security governance program," noting that the OPM failed to fill key cyber security leadership positions. The absence of leadership meant that the OPM did not have the necessary oversight to correct system-wide cyber security issues. In addition, the OIG found that the OPM lacked evidence that all laptops issued to OPM employees had encryption capability, so laptops with sensitive PII may have been particularly vulnerable to hackers.

54. In 2010, the OIG again found a "material weakness" in the OPM's cyber security governance, meaning that the OPM's employees did not have guidance on how to prevent software systems from being hacked. In addition, the OIG added Security Assessment and Authorization[8] as a material weakness finding that the quality of the authorization process had worsened from the previous two years. The OIG noted that the OPM lacked the staff to ensure that all software systems had cyber security measures necessary to fend off cyber-hacks.

55. In 2011, the OIG again labeled the OPM's cyber security governance a "material weakness," noting that the OPM continued to lack staff in key cyber security leadership positions, and that the DSO's did not have the technical skill to effectively determine whether a software system was vulnerable to an attack. In addition, the OIG recognized that the authorization process remained inconsistent between different departments, meaning that while some departments were determining which software systems met security standards, other departments were unable to recognize if a software system was vulnerable to attack.

56. In 2012, the OIG continued to recognize a "material weakness" in the OPM's cyber security governance, finding that though the OPM had hired a Chief Information Security Officer ("CISO")—a key leadership position in its cyber security team—the OPM did not give the CISO any authority to oversee the DSOs. This meant the new position failed to centralize the OPM's security personnel and provide an oversight structure to ensure that software systems were secure. The OIG also found that there were "numerous [cyber] security incidents [] that led to the loss or unauthorized release of mission-critical or sensitive data." For example, the Heritage Foundation reported that in May 2012, an unknown hacker broke into the OPM and posted thirty-seven user IDs and passwords online. The OIG also found that when employees

---

[8] In 2010, the OIG labeled this process Certification and Accreditation.

accessed software systems using a remote access session—where the employee can use a computer to log into the software system from a remote location such as a laptop in a public place—the remote access would not terminate if the user failed to log off. If an employee failed to sign off, other parties could access the system from the same computer without having to enter log-in credentials.

57. In 2013, despite years of documented problems regarding cyber security governance at the OPM, the OIG concluded that "[l]ittle progress was made" to address the lack of "a centralized security management structure," and therefore expressed its doubt as to the OPM's ability to manage major software systems. The OIG also found that the OPM failed to require PIV authentication for any of the 47 major applications, meaning that if a hacker obtained an employee's password, the hacker could access the system without the extra protection afforded by the PIV card.

58. According to technology news source Ars Technica—quoting Vinny Troia, the director of risk and security consulting at McGladrey, LLP—the OPM's recidivism was intentional and a direct result of the fact that "[t]here was no consequence for systems breaking the law." The OIG's 2014 report specifically cited the lack of any consequences for not complying with FISMA as a contributing cause to delays in getting the systems up to specifications.

59. In its 2014 audit report, the OIG similarly found that the 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." As a result, in 2014, the OIG recommended introducing administrative sanctions to combat instances of willful non-compliance with FISMA requirements. The OIG further recommended

"that the performance standards of all OPM major system owners be modified to include a requirement related to FISMA compliance for the systems they own."

E. The OPM's History of Software System Hacks

60. The OPM was on notice of its critical system deficiencies as a result not only of the OIG's persistent warnings going back to 2007, but also through a number of actual breaches in recent years leading up to the OPM Breach that is at issue here. Indeed, such breaches not only laid bare the dramatic gaps in OPM's data security, but each breach itself makes the OPM even more vulnerable to further breaches, because passwords and other information that can be used to gain even greater access are already in the hands of the hackers, making a subsequent breaches on a larger scale more likely and more dangerous. The OPM nevertheless ignored the gravity of situation and continued on with business as usual, making the OPM Breach essentially inevitable given the laxity of the security measures being taken.

61. For example, in July 2014, the New York Times publicized an attempted OPM intrusion that the agency had been investigating since March 2014. Hackers reportedly operating from mainland China broke into the OPM's computer networks, and targeted files of thousands of employees applying for security clearances. The hackers gained access to some of the databases before the federal authorities detected the threat and blocked them from the network. Shortly after the article was published, the OPM sent an email to its employees assuring that it had not identified any loss of PII.

62. In August 2014, media sources revealed that US Investigations Services LLC ("USIS"), a contractor that provided the bulk of background checks for federal security clearances—including for the OPM—had been hacked, potentially exposing thousands of government employee records. In a public statement, the company said the "attack has all the markings of a state-sponsored attack." After the breach, the OPM terminated contracts with

USIS. Former Undersecretary for Management of Homeland Security Chris Cummiskey stated that the OPM's response to the hack lacked coordination and, "[w]e've seen this a couple of times now and unfortunately we act like each iteration is the first time it's ever occurred." In testimony before the House of Oversight and Government Reform Committee regarding the 2014 USIS breach, the OPM's Chief Information Officer Donna Seymour ("Seymour") acknowledged both USIS and the OPM were attacked by hackers in March 2014, but claimed they were able to "put mitigations in place to better protect the situation."

F. The KeyPoint Hack

63. In December 2014, the 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"). Nathaly Arriola, the OPM's spokesperson, stated that there was "no conclusive evidence to confirm sensitive information was removed from the [software] system."

64. KeyPoint became the largest government contractor performing private employee clearances after its predecessor, USIS, was terminated after the cyber-attack it experienced in 2014. According to reports, "KeyPoint moved quickly to fill the void, looking to double the size of its investigative workforce." However, because USIS's caseload was significant and involved 21,000 background checks a month, there was widespread skepticism that any entity could cover the workload on "short notice." Without due care, 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.

65. In the wake of the KeyPoint Hack, and in view of the OPM Breach, it has become clear that KeyPoint and the OPM grossly mishandled the transition and failed to protect Plaintiff and Class members' PII and other confidential information in an adequate and secure manner.

Even today, KeyPoint has been unable to identify how the breach it announced in December 2014 happened. The reason it can't—according to Ann Barron- DiCamillo (director of the DHS U.S. Computer Emergency Readiness team)—is due to "lack of logging." In other words, according to one report, KeyPoint never set up logs to track the malware deployed to infiltrate its systems and therefore simply doesn't know what happened.

66. Following the KeyPoint hack, the DHS and other agencies began helping the OPM with its network monitoring. According to DHS spokesman S.Y. Lee, DHS and "interagency partners" were helping the OPM improve its network monitoring "through which [the] OPM detected new malicious activity affecting its [software] systems and data in April 2015." The DHS and "interagency partners" used a security monitoring program to discover a potential breach. According to Lee, "DHS concluded at the beginning of May 2015 that [the] OPM data had been compromised." DHS determined that the event wasn't just historical, but an ongoing breach of the OPM's software systems and data center.

67. After announcement of the KeyPoint Hack, Seymour—in an e-mail to colleagues at the OPM—praised the OPM's commitment to cyber-security measures, stating: "security of our networks and the data entrusted to us remains our top priority. This incident serves as yet another reminder that we all must be ever-vigilant in our efforts to understand, anticipate and guard against the threat of cyber-attacks." During this same time period, however, the OPM was not in compliance with the FISMA or the OIG's recommendations and had not been for years.

G. The OPM Breach

68. On June 4, 2015, the OPM announced it would notify approximately 4 million current and former federal applicants and employees in the executive branch 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, the OPM admits that it detected the intrusion as early as April.

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

69. In order to access the OPM's database, hackers installed a malware package that industry analysts opine was likely delivered via an e-mail "phishing"[9] attack within the OPM's software systems through which the hackers gained access to valid OPM user credentials. 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 sneak data out of the network over the Internet, hiding its activity internally among normal traffic. It was only when the OPM was assessing its software systems to actually implement continuous monitoring tools, as required by FISMA, that it discovered that something was wrong.

70. 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.

---

[9] Phishing is the attempt to acquire sensitive information such as usernames and passwords by masquerading as a trustworthy entity in an electronic communication. An example would be an attacker who sends an email to an employee purportedly on behalf of the employer's IT department, but which includes a link back to a website controlled by the attacker.

71. On July 9, 2015, the OPM confirmed a "separate but related cybersecurity incident[]" that affected 22.1 million individuals. The OPM's news release stated that the 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."

72. The 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."

73. The identity of the individuals or entity responsible for the cyber-attack on the OPM, and details confirming exactly how adversaries conducted the attack, remain classified. Many officials, including U.S. Intelligence Chief James Clapper, have attributed the attack to China. However, a report by the Institute for Critical Infrastructure Technology ("ICIT"), a bipartisan forum of Federal Agency executives, legislative and industry leaders focused on IT

security issues, states that "[g]iven the lack of sophistication of the attack, the shabby defenses of OPM's critical systems, and the immense value of the exfiltrated assets, almost any known actor group would have seized the opportunity to breach OPM if they had the knowledge of their internal systems and the resources to conduct the breach."

74. After the breach was detected, the OPM failed to disclose in a timely or adequate manner the facts surrounding how the breach happened, why it happened, who was affected, and what was stolen. Moreover, OPM and KeyPoint have pointed fingers at each other, each refusing to accept responsibility for the security failures and passive-aggressively blaming the other. Most recently, the OPM has sought to shift blame for the OPM Breach to KeyPoint. former OPM Director Katherine Archuleta ("Archuleta") recently stated that "the adversary leveraged a compromised KeyPoint user credential to gain access to [the] OPM network," though she stopped short of saying the company was "responsible or directly involved in the intrusion." KeyPoint President and CEO Eric Hess responded to Archuleta's claims by denying all culpability: "I would like to make clear that we have seen no evidence suggesting KeyPoint was in any way responsible for the OPM breach." He then shifted blame back to the OPM: "[t]o be clear, the employee was working on OPM's systems, not KeyPoint's."

75. The OPM continues to insist it did nothing wrong. Archuleta stated that "if anyone is to blame, it is the perpetrators." But 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 which are ***mandated*** by federal law. Moreover, Archuleta's decision not to shut down many of the critically vulnerable OPM's software systems in late 2014—in contravention of the OIG's recommendation—further led

directly to the OPM Breach. The ICIT stated that "OPM effectively handed away the keys to the castle by maintaining an undefended cybersecurity posture."

H. Subsequent Investigations Confirm OPM's Culpability in the Data Breach

76. Even prior to the recent July 9, 2015 announcement, the facts surrounding the OPM breach overwhelmingly demonstrate the agency's direct responsibility for the theft of more than 21 million Americans' highly sensitive PII.

77. According to the ICIT, "the OPM breach was not a sophisticated attack. The failure of DHS or OPM systems to detect the breach does not indicate a level of sophistication on behalf of the adversary; rather, it only shows that the breach was sophisticated [given that] applications … have not been updated since the Y2K bug." Covenant Security Systems President and Founder Danyetta Fleming Magana remarks that "it appears as though this was the equivalent of a car thief politely asking for the car keys and once handed them drove the car for over a year before being noticed."

78. At the Committee Hearing, Chairman Jason Chaffetz, U.S. Representative for Utah's 3rd congressional district told Archuleta, "you failed. You failed utterly and totally." Chaffetz stated that the breach should "Come as no surprise given [the OPM's] troubled track record." Chaffetz compared the breach to "leaving all the doors and windows open in your house and expecting that nobody" would come in take anything.

79. House Representative Ted Lieu called for Archuleta to resign, stating that "[i]n national security it's got to be zero tolerance, that's got to be the attitude. We can't have these breaches." He added, "[i]n the past when we've had this, leadership resigns or they're fired . . . Send a signal that the status quo is not acceptable. We cannot continue to have this attitude where we make excuse after excuse."

80. House Representative Steve Russell stated that the OPM's failure to encrypt data was "absolute negligence that puts the lives of Americans and also foreign nationals at risk."

81. On July 10, 2015, one day after revealing that more than 22 million people had their data stolen in a pair of massive cyber attacks on the agency, Archuleta announced her resignation as director of the OPM.

82. In the OPM Breach, the hackers stole eOPF files that contain employee performance records, employment history, employment benefits information, federal job applications, resumes, 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."

83. 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 for identity theft 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 they want 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.

84. In testimony before the Subcommittee on Information Policy, Census and National Archives Committee on Oversight and Government Reform: Identity Theft, Daniel Bertoni, Director of the United States Government Accountability Office ("GAO") stated that, "[m]any 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, "in [one] year, as many as 10 million people – or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion."

85. Already, hackers are taking advantage of the OPM's breach. Following announcement of the initial breach, the OPM emailed employees whose information was compromised and offered credit monitoring services through a link in the email. These emails were quickly duplicated by hackers, and used to send phishing emails attempting to trick employees into handing over account logins and other personal information, much in the same way that the hackers obtained information in the original OPM Breach. Both the authentic and duplicated emails told employees to click on a link to register for credit monitoring services. According to the Washington Post, computer experts have noted that the OPM could be "putting federal [software] systems in jeopardy again by asking employees to click on links in the

emails." Another report similarly noted, "[i]t's little short of appalling that for a week the OPM sent out emails telling recipients to click on an embedded link to register for their credit monitoring services. This opened the door wide for phishing attacks."

86. The records stolen in the OPM Breach also have national security implications. The hackers accessed EPIC, a background investigation toolset, and stole 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 and a senior vice president at ICF International. "It's really a personal document." Or, as Representative Stephen Lynch expressed during a congressional hearing into the OPM breaches, the SF-86 "ask[s] them everything: what kind of underwear they wear, you know what kind of toothpaste they -- I mean it's a deep dive. . . . They hacked this ...They got this information on Standard Form 86. So they know all of these employees who -- and everything about them that we ask them in the Standard Form 86."

87. Log-in credentials stolen in the OPM Breach are reportedly already 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 log-in 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."

V. PLAINTIFF'S DAMAGES

88. Plaintiff and millions of other Class members have been seriously and identically harmed by the OPM's mishandling of their sensitive PII. The damage here has already been done. 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.

89. 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:

- out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- 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;
- 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 the OPM for the purpose of deriving employment from the OPM and with the understanding that the OPM and its contractors 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;
- 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, which remains in the OPM's possession and is subject to further breaches so long as the OPM fails to undertake appropriate and adequate measures to protect the PII in its possession; and
- continued risk associated with government-issued identification, including without limitation Social Security cards, passports, naturalization numbers, military service numbers and visas.

90. The token remedy offered by the OPM – credit monitoring for 18 months, plus $1 million in identity theft insurance and identity restoration services through December 7, 2016 – is woefully inadequate to protect against or compensate victims for these risks for at least four reasons.

91. ***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 more robust features of a premium three-bureau, modern identity service, which is unfortunately necessary in this instance due to the breadth of the information compromised in the OPM Breach.

92. However, even traditional credit monitoring, when at its best (all three bureau reports, 3-bureau monitoring), 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. But 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

synthetic identity theft,[10] identity theft of medical information or insurance information, or theft of professional credentials. Thieves also frequently target breach victims with malware, phishing attacks, and "key-logger" attacks.[11] Thieves frequently use mobile payment and social media sites and newer forms of credit payment like Amazon and EBay for committing fraud. 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.

93. ***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.

94. ***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 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

---

[10] 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.

[11] A "key-logger" attack records every key-stroke that is entered into the target's computer and transmits that information to the attacker without the user's knowledge, thus providing access to passwords and any other sensitive information entered by the user.

suggests that this information already has been, and continues to be, bought and sold on the black market.

95. ***Finally***, the 18-month duration of services currently offered by the 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 5 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.

VI. CLASS ACTION ALLEGATIONS

96. **Class Definition**. 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 the OPM on June 4, 2015 and July 9, 2015.***

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

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

99. 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 can only be ascertained through appropriate discovery, there are at least 22 million members of the class

located throughout the United States. It would be impracticable to join the class members individually.

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

(i) whether the OPM's conduct violated the Privacy Act of 1974;

(ii) whether the 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;

(iii) whether the OPM disclosed Plaintiff and Class members' PII without their prior written consent;

(iv) whether the Defenants' conduct was willful or with flagrant disregard for the security of Plaintiff and Class Members' PII;

(v) whether the Defendants' conduct was negligent;

(vi) whether the OPM's conduct violated the Administrative Procedure Act;

(vii) whether Defendants had a legal duty to use reasonable cyber security measures to protect Plaintiff and Class members' PII;

(viii) whether Defendants breached its legal duty by failing to protect Plaintiff and Class members' PII;

(ix) whether Defendants acted reasonably in securing Plaintiff and Class members' PII;

(x) whether Plaintiff and Class members are entitled to damages, declaratory and/or injunctive relief.

101. 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 all 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 the OPM.

102. 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 intends to pursue this action vigorously. Plaintiff has no interests contrary to or in conflict with the interests of class members.

103. 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.

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

(i) 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;

(ii) 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;

(iii) 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

(iv) The claims of class members are comprised of common issues that are appropriate for certification under Rule 23(c)(4).

VII. CLAIMS

COUNT I
VIOLATIONS OF THE PRIVACY ACT OF 1974 (5 U.S.C. § 552A)
(On behalf of Plaintiff and Class members against the OPM)

105. Plaintiff incorporates each and every allegation above as if fully set forth herein.

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

107. 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 . . . ."

108. 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."

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

110. The 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)."

111. The OPM is, and at all relevant times was required by law to comply with both FISMA and the Modernization Act. The 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.

112. However, dating back to at least 2009, through a continuous course of conduct, the OPM intentionally and willfully failed to comply with FISMA and demonstrated multiple "significant deficiencies." The OPM thus 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 the OPM's noncompliance with FISMA. The OIG explicitly recognized that the OPM failed to comply with FISMA each year from 2009-2014:

- **2009.** "The continuing weaknesses in OPM's information security program result directly from inadequate governance. Most, if not all, of the exceptions we noted this year resulted from a lack of necessary leadership, policy, and guidance."

- **2010.** "We continue to consider the IT security management structure, insufficient staff, and the lack of policies and procedures to be a material weakness related to the management of OPM's Certification and Accreditation (C&A) process. The C&A concerns were reported as a significant deficiency in the FY 2008 and FY 2009 [FISMA] audit reports."

- **2011.** "We continue to believe that information security governance represents a material weakness in OPM's IT security program. . . . [T]here were, in our opinion, three root causes of OPM's C&A issues: insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized DSO model in place at OPM."

- **2012.** "Throughout FY 20-12, the OCIO continued to operate with a decentralized IT security structure that did not have the authority or resources available to adequately implement the new policies . . . . Th[is] material weakness remains open in this report, as the agency's IT security function remained decentralized throughout the FY 2012 FISMA reporting period and because of the continuing instances of non-compliance with FISMA requirements."

- **2013.** "The findings in this audit report highlight the fact that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

- **2014.** "The findings in this audit report . . . indicate that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements."

113. Specifically, the OPM was required—but failed—to take several steps to comply with applicable security rules and regulations including but not limited to:

- Implementing PIV multi-factor authentication for all 47 of the agency's major applications, as required by the OIG's prior audit reports and required by OMB Memorandum M-11-11;

- Centralizing its cyber security structure to ensure that it can effectively manage its cyber security program and protect its software systems against a breach; and . Shutting down unauthorized software systems and ensuring that all software systems are authorized before being put back into operation.

114. The OIG found that one of the "core causes" of the OPM's non-compliance with FISMA was the "fact that there are currently no consequences for OPM systems that do not have a valid Authorization to operate." As a result, in 2014, the OIG recommended introducing administrative sanctions to combat instances of willful non-compliance with FISMA requirements.

115. From 2009 to 2014, the OIG also found that the OPM was not in compliance with several standards promulgated under 40 U.S.C. § 11331, as is required by FISMA, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, contractor systems, security capital planning, and contingency planning.

116. Through a continuous course of conduct, the 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."

117. The OPM's history of non-compliance with FISMA's legal requirements that culminated in the 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.

118. As a result of the 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 the OPM for the purpose of deriving employment from the OPM and with the understanding that the 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 the OPM's possession and is subject to further breaches so long as the 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)(1)(D) and (g)(4).

COUNT II
VIOLATIONS OF THE ADMINISTRATIVE PROCEDURE ACT (5 U.S.C. § 701, *et seq.*)
(On behalf of Plaintiff and Class members against the OPM)

119. Plaintiff incorporates each and every allegation as if fully set forth herein.

120. The 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 the 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, the 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.

121. The 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 the 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 the OPM's noncompliance with FISMA and the Modernization Act resulted in the Privacy Act violations at the center of this lawsuit

122. The 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 the OPM to bring its cyber security systems in compliance with FISMA, but each year, the 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 the 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."

123. The 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 the OPM shut down "[software] systems that do not have a current and valid authorization." However, the OPM refused to shut down its software systems. At the Committee Hearing, Archuleta stated

that, "[i]t 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."

124. The 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 the OIG'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 the OPM's willful and intentional continuous course of conduct resulted in the OPM Breach in which Plaintiff's and Class members' PII was compromised, the OPM's continuous string of decisions not to comply with FISMA caused violations the Privacy Act and damages to Plaintiff and Class members.

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

126. The 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 the 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.

127. Because of the OPM's decisions not to comply with FISMA, the 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.

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

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

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

130. Plaintiff incorporates each and every allegation as if fully set forth herein.

131. 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.

132. 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.

133. 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 the OPM and its contractors, and yet KeyPoint

failed to take reasonable precautions to safeguard the PII of federal applicants and related non-applicants.

134. In December 2014, the 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 which compromised the PII of approximately 22 million individuals.

135. 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.

136. But for KeyPoint's failure to implement and maintain adequate security measures to protect Plaintiff'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.

137. 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 varieties of serious fraud.

138. 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 the OPM and KeyPoint for the purpose of deriving employment from the OPM and with the

understanding that the 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 the OPM's possession and is subject to further breaches so long as KeyPoint and the 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.

VIII. 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.

IX. JURY DEMAND AND DESIGNATION OF PLACE OF TRIAL

Plaintiff hereby demands a trial by jury of all issues properly triable.

Dated: August 14, 2015

Respectfully submitted,

SANDS ANDERSON PC

/s/ J. Jonathan Schraub
J. Jonathan Schraub (DC Bar No. 950816)
Paige Levy Smith (DC Bar No. 453535)
1497 Chain Bridge Road
Suite 202
McLean, VA 22101
(703) 893-3600
(703) 893-8484 (facsimile)
plevy@sandsanderson.com
jjschraub@sandsanderson.com

LABATON SUCHAROW LLP

/s/ Joel H. Bernstein
Joel H. Bernstein (*Pro Hac Vice Forthcoming*)
Garrett Bradley (*Pro Hac Vice Forthcoming*)
Corban S. Rhodes (*Pro Hac Vice Forthcoming*)
140 Broadway
New York, NY 10005
(212) 907-0700
(212) 818-0477 (facsimile)
jbernstein@labaton.com
gbradley@labaton.com
crhodes@labaton.com

Counsel for Plaintiff and the Class