Philip C. Monrad (State Bar No. 151073)
Jennifer Keating (State Bar No. 250857)
LEONARD CARDER, LLP
1330 Broadway, Suite 1450
Oakland, CA 94612
Tel: (510) 272-0169
Fax: (510) 272-0174
Email: pmonrad@leonardcarder.com
Email: jkeating@leonardcarder.com

Gregory O'Duden (DC Bar No. 254862)
Larry J. Adkins (DC Bar No. 425653)
Paras N. Shah (DC Bar No. 983881)
Allison C. Giles (DC Bar No. 439705)
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Fax: (202) 572-5645
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

(Applications for pro hac vice admission pending)

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO AND OAKLAND DIVISION

NATIONAL TREASURY EMPLOYEES UNION, STEPHEN HOWELL, JOHN ORTINO, Plaintiffs, v. KATHERINE ARCHULETA, Director, Office of Personnel Management Defendant.	Case No. 15-3144 **COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

INTRODUCTION

This action seeks a remedy for the unconstitutional disclosure by the federal government of the personal information of members of the National Treasury Employees Union (NTEU) currently or formerly employed by the federal government. When the government collected the information in question, it assured the individuals who provided the information that it would be safeguarded and kept confidential. On June 4, 2015, the Office of Personnel Management (OPM) announced that it had become aware of a breach in its data systems, resulting in unauthorized access to the personal information of more than four million (4,000,000) current and former federal employees, including numerous NTEU members. According to OPM, the types of information that may have been compromised include name, Social Security number, date and place of birth, and current and former addresses. OPM notified thousands of NTEU members that their personal information was compromised by this data breach.

OPM cautioned that, as its investigation continued, additional exposure could be discovered. On June 12, 2015, OPM announced that it had discovered a second breach. This breach resulted in unauthorized access to data systems containing materials related to the background investigations of current, former, and prospective federal employees.

Among the materials compromised in this second breach were an unknown number of completed Standard Form 86's (SF-86). The SF-86 (Questionnaire for National Security Positions) is a form that individuals complete in order to be considered for or retained in national security positions as defined in 5 C.F.R. Part 732 and to obtain access to classified information under Executive Order 12968.

Because OPM announced that this second breach affected background investigation materials, Plaintiffs reasonably believe that the compromised materials also included an unknown number of completed Standard Form 85's (SF-85) and Standard Form 85P's (SF-85P). The SF-85 (Questionnaire for Non-Sensitive Positions) is a form that individuals complete as part of a background investigation to determine whether they, as applicants or incumbents, are suitable for federal employment. The SF-85P (Questionnaire for Public Trust Positions) is a form that individuals complete as part of background investigations to determine whether they,

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

as applicants or incumbents, are suitable for federal employment in "public trust" or "sensitive" positions, as defined in 5 C.F.R. Part 731.

Completed SF-85's, SF-85P's, and SF-86's contain personal information relating to the individual completing the form and to that person's relatives, friends, and others. To date, OPM has not announced the number of individuals affected by this second breach.

These massive data breaches came after OPM had been put on notice of deficiencies in its information security practices by OPM's Office of Inspector General (OIG). Over a period of many years, the OIG had identified numerous significant deficiencies, including deficiencies related to OPM's decentralized security governance structure, its failure to ensure that its information technology systems met applicable security standards, and its failure to ensure that adequate technical security controls were in place for all servers and databases.

Although on notice of serious flaws in its data system security, OPM failed to adequately secure personal information in its possession--a failure that was reckless under the circumstances. OPM's reckless failure to safeguard personal information to which it had been entrusted resulted in the unauthorized disclosure of NTEU members' personal information in violation of their right, under the U.S. Constitution, including the Due Process Clause of the Fifth Amendment, to informational privacy. Plaintiffs seek a declaration that OPM's conduct was unconstitutional and other equitable relief.

JURISDICTION

1. This Court has jurisdiction pursuant to 28 U.S.C. § 1331.

VENUE AND INTRADISTRICT ASSIGNMENT

2. Venue is proper in this District pursuant to 28 U.S.C. § 1391(e). Venue is proper in the San Francisco-Oakland Division under Local Rule 3-2 because NTEU has a field office in Oakland, California, and has many members who reside or work within the Division who were affected by the OPM data breaches described in this complaint; Plaintiffs Howell and Ortino reside within the Division; and Plaintiff Ortino works within the Division. Thus, Plaintiffs' respective injuries have occurred, at least in substantial part, within the Division.

///

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

PARTIES

3. Plaintiff National Treasury Employees Union (NTEU) is an unincorporated association with its principal place of business at 1750 H Street, N.W., Washington, D.C. 20006. Pursuant to Title VII of the Civil Service Reform Act, Public Law No. 95-454, 92 Stat. 1111, NTEU is the exclusive bargaining representative of approximately 150,000 federal employees in 31 federal agencies, including thousands of dues-paying members whose personal information has been compromised. NTEU represents the interests of these employees by, inter alia, negotiating collective bargaining agreements; arbitrating grievances under such agreements; filing unfair labor practices; lobbying Congress for favorable working conditions, pay, and benefits; and enforcing employees' collective and individual rights in federal courts. NTEU brings this action in its representative capacity on behalf of its members who have been injured by the Defendant's failure to protect their personal information.

4. Plaintiff Stephen Howell resides in Pleasanton, CA (Alameda County). He is employed by the Internal Revenue Service (IRS) in San Jose, CA, as an Appeals Officer. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU.

5. Plaintiff John Ortino resides in Burlingame, CA (San Mateo County). He is employed by Customs and Border Protection in San Francisco, CA, as a Customs and Border Protection Officer. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU.

6. Defendant Katherine Archuleta is Director of OPM. The Director is responsible for executing, administering, and enforcing civil service laws and regulations, including the requirement that Federal government applicants and employees undergo background investigations. The Director is also responsible for ensuring that personal information entrusted to OPM is protected from unauthorized disclosure. The Director is sued solely in her official capacity.

///

///

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

STATEMENT OF CLAIMS

OPM's Data Collection and Retention

7. In its role as the federal civil service's personnel manager, OPM collects and stores immense amounts of federal employee data. It manages a software system that provides internet-based access to employee personnel folders. That system is called the electronic Official Personnel Folder (eOPF), and its contents include employee performance records, employment history, benefits, job applications, resumes, education transcripts, and birth certificates.

8. OPM conducts over two million background investigations a year. These investigations, which are required by Executive Orders and other rules and regulations, are used by the federal government to make suitability and security clearance determinations.

9. OPM uses a variety of database systems as part of its investigative function, including those discussed in this paragraph. It uses a web-based automated software system to process standard investigative forms used for background investigations: the Electronic Questionnaires for Investigations Processing (e-QIP). eQIP is intended to allow for the secure transmission of personal investigative data to the requesting agency. OPM's Personal Investigations Processing System (PIPS) is a background investigation software system that handles individual investigation requests from agencies. It contains an index of background investigations conducted on federal employees. OPM's Central Verification System (CVS) contains information on security clearances, investigations, suitability determinations, background checks for those seeking access to federal facilities, and polygraph data.

The First Breach

10. OPM experienced a cybersecurity incident, which it announced on June 4, 2015, that compromised the personal information of approximately 4 million individuals. OPM's announcement also stated that it would send notifications to the affected individuals.

11. OPM detected the incident in April 2015.

12. After discovering the intrusion announced on June 4, 2015, OPM publicly stated that, since its investigation was on-going, additional exposures of personal information could be discovered.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

13. On or about June 9, 2015, OPM posted on its website a set of "Frequently Asked Questions" (FAQ) that included information about this data breach. One of the FAQ's read as follows:

> What personal information was compromised
>
> OPM maintains personnel records for the Federal workforce. The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, and current and former addresses. It is the type of information you would typically find in a personnel file, such as job assignments, training records, and benefit selection decisions, but not the names of family members or beneficiaries and not information contained in actual policies. The notifications to potentially affected individuals will state exactly what information may have been compromised.

14. An as yet unknown number of NTEU members were determined by OPM to have been affected by this first data breach and have received the notification described in Paragraphs 10 and 13.

The Second Breach

15. Based on OPM's public announcements, Plaintiffs reasonably believe that OPM systems, such as those discussed in Paragraph 9, containing, among other information, information related to the background investigations of current, former, and prospective Federal government employees, and those for whom a Federal background investigation was conducted, were subject to unauthorized access, resulting in the taking of that information.

16. As part of the background investigations described in Paragraph 8, federal employees and applicants are required to submit forms such as the Standard Form 85 (Questionnaire for Non-Sensitive Positions) (SF-85); Standard Form 85P (Questionnaire for Public Trust Positions) (SF-85P); and Standard Form 86 (Questionnaire for National Security Positions) (SF-86).

17. A completed, current version of the SF-85 (Form Approved OMB No. 3206-0261) can contain, inter alia, the following information about the individual who has completed

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

it: Social Security number; citizenship; prior addresses; education; employment history; information about persons who know the individual well; selective service record; military history; and whether the individual has used, possessed, supplied, or manufactured illegal drugs.

18. The current version of the SF-85 includes an "Authorization for Release of Information" to authorize background investigators "to obtain any information relating to [the individual's] activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, retail business establishments, or other sources of information to include publically available electronic information. This information may include, but is not limited to, [the individual's] academic, residential, achievement, performance, attendance, disciplinary, employment history, and criminal history record information."

19. Including instructions, the current online version of the SF-85 is eight pages in length.

20. In addition to information contained on the SF-85, a completed, current version of the SF-85P (Form Approved OMB No. 3206-0191) can also include marital status information; information about relatives; information about previous background investigations; foreign countries visited; police record; and financial history.

21. The current version of the SF-85P includes an "Authorization for Release of Information" similar in its coverage to that included in the SF-85, except that the SF-85P release also allows investigators to collect financial and credit information.

22. The current version of the SF-85P includes an "Authorization for Release of Medical Information" that, when signed, permits an investigator to ask the individual's health care practitioner the following three questions about the individual's mental health:

> Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability?
>
> If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

What is the prognosis?

23. The current version of the SF-85P includes a "Supplemental Questionnaire for Selected Positions" with additional questions about the use of illegal drugs and drug activity; the use of alcohol; and the individual's mental health history.

24. Including instructions, the current online version of the SF-85P is 12 pages in length.

25. A completed, current version of the SF-86 (Form Approved OMB No. 3206 0005) can contain, inter alia, the following information about the individual who has completed it: Social Security number; passport information; citizenship; previous residence information; education; employment history; selective service record; military history; persons who know the individual well; marital status; relatives; foreign contacts; foreign activities; foreign business, professional activities, and government contacts; foreign travel; psychological and emotional health; police record; illegal use of drugs and drug activity; use of alcohol; government investigation and clearance record; financial record; use of information technology systems; involvement in non-criminal court actions; and association record.

26. The current version of the SF-86 includes an "Authorization for Release of Information" similar in content to authorization described in Paragraph 21 for the SF-85P.

27. The current version of the SF-86 includes an "Authorization for Release of Medical Information Pursuant to the Health Insurance Portability and Accountability Act (HIPAA)" similar in content to the authorization described in Paragraph 22 for the SF-85P.

28. Including instructions, the current online version of the SF-86 is 127 pages in length.

29. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Director Archuleta confirmed that persons who had filed SF-86 had been affected by the breach by answering the following question from Rep. Chaffetz concerning the scope of the cyber intrusion:

Q: Does it include anybody who's filled out SF-86, the standard form 86?

A: The individuals who have completed an SF-86 and – may be included in that. We can provide any additional information in a classified setting.

OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 14 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management), available at www.fednews.com.

30. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Donna Seymour, OPM Chief Information Officer, confirmed that persons who had filed SF-86s had been affected by the breach by answering the following question from Rep. Cummings:

Q: What can you tell us about the type of personal information that was compromised in this breach?

A: The type of information involved in the personnel records breach [the "First Breach"] includes typical information about job assignment, some performance ratings, not evaluations, but performance ratings, as well as training records for our personnel. The information involved in the background investigations incident [the "Second Breach"] involves SF 86 data, as well as clearance adjudication information.

Id. at 16 (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Management).

31. During her June 16, 2015 testimony, Ms. Seymour confirmed that information related to affected individuals' entire careers had been affected by answering the following questions from Rep. Cummings:

Q: Ms. Seymour, it was reported on Friday that in addition to this breach, hackers had breached highly sensitive information gathered in background investigations of current and former federal employees. Is that true?

A: Yes, sir, that is.

Q: Do you know how far back that goes?

A: No, sir, I don't. These are – the issue is that these are longitudinal records, so they span an employee's you know, career. And so I do not know what the oldest record is.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

Q: So, it's possible that somebody could be working for the federal government for 30 years. And their information over that 30 years could've been breached?

A: Yes, sir. These records do span an employee's career.

Id.

OPM's Failure to Protect Plaintiffs' Personal Information

32. The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et. seq., makes the head of each agency, including the Defendant, responsible for providing information security protections and ensuring that agency officials take steps to reduce the risk of unauthorized use of information in the agency's possession.

33. FISMA further provides that each agency head, including the Defendant, is responsible for complying with the requirements of the statute and pertinent information technology policies, procedures, standards, and guidelines established by appropriate authorities.

34. As the Inspector General reports and testimony discussed below demonstrate, Defendant failed to satisfy her responsibilities under FISMA and other applicable authority, a failure that is relevant because it is illustrative of Defendant's broader reckless disregard of Plaintiffs' informational privacy rights.

35. As recorded in a June 16, 2015 written statement submitted to the House Committee on Oversight and Government Reform, when Director Archuleta was sworn in 18 months earlier, she "immediately became aware of security vulnerabilities" in OPM's systems. OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 6 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management), available at www.fednews.com.

36. Director Archuleta repeated the assertions described in Paragraph 35 in a written statement submitted to the Senate Subcommittee on Financial Services and General Government. Federal IT Spending/OPM Data Security: Hearing Before the Subcommittee on Financial Servs. and General Government, Senate Comm. on Appropriations, 114th Cong. 4-5 (2015) (Statement of Katherine Archuleta, Director, Office of Personnel Management).

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

37. In its audit report for Fiscal Year 2014, required by FISMA, OPM's Office of the Inspector General documented numerous deficiencies in OPM's information technology (IT) security program and practices. Office of Personnel Management, Office of Inspector General, Audit Report 4A-C1, 00-14-016 (Nov. 12, 2014).

38. In a June 16, 2015 written statement submitted to the House Committee on Oversight and Government Reform, OPM Assistant Inspector General for Audits, Michael R. Esser, described the audits of OPM's information technology security programs and practices that his office had performed under FISMA. OPM: Data Breach: Hearing Before the House Comm. on Oversight and Gov't Reform, 114th Cong. (2015) (statement of Michael Esser, Asst. Inspector General for Audits, Office of Personnel Management), available at www.democrats.oversight.house.gov/legislation/hearings/full-Committee-hearing-OPM-data-breach (hereinafter "Esser Statement").

39. In his June 16, 2015 written statement, Mr. Esser described some of the problems identified in these audits as dating back to Fiscal Year 2007. Id. Mr. Esser identified three of the "most significant issues identified in our FY 2014 FISMA audit" as being "Information Security Governance," "Security Assessment and Authorization," and "Technical Security and Controls." Id.

40. In his June 16, 2015 written statement, Mr. Esser described "Information Security Governance" as the "management structure and processes that form the foundation of a successful technology security program." Id. He described a "material weakness," defined as "a severe control deficiency that prohibits the organization from adequately protecting its data," in OPM's security governance practices. Id. First identified as a material weakness in the Fiscal Year 2007 report, his office "continued to identify this security governance issue as a material weakness in all subsequent FISMA audits through FY 2013." Id. Although his office's Fiscal Year 2014 report classified this issue as a less serious "significant deficiency," he stated that OPM "continues to be negatively impacted by years of decentralized security governance" causing its technical infrastructure to remain "fragmented and therefore inherently difficult to protect." Id.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

41. In his June 16, 2015 written statement, Mr. Esser described "Security Assessment and Authorization" as a "comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment." Id. He stated that the "Office of Management and Budget (OMB) mandates that all Federal information systems have a valid Authorization." Id. After being removed as a concern in the FY 2012 audit report, problems recurred such that in FY 2014, "21 OPM systems were due for an Authorization, but 11 of those were not completed on time and were therefore operating without a valid Authorization." Id. Because they were operating without Authorization, his office recommended that these eleven systems be shut down, but none were shut down. Id.

42. In his June 16, 2015 written statement, Mr. Esser noted that two of the eleven OPM systems operating without an Authorization were general support systems on which "over 65 percent of all systems operated by OPM" reside. Id. at 4. Two others are owned by OPM's Federal Investigative Service, which, Mr. Esser, explained, "is responsible for facilitating background investigations for suitability and clearance determinations." Id. Mr. Esser's office believed that "the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program." Id.

43. In his June 16, 2015 written statement addressing "Technical Security Controls," Mr. Esser referred to 29 audit recommendations in the Fiscal Year 2014 FISMA report and stated that "two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication of IT systems using personal identity verification (PIV) credentials." Id.

44. In his June 16, 2015 written statement, Mr. Esser described "configuration management" as referring to the "policies, procedures, and technical controls used to ensure that IT systems are securely deployed." Id. His office's Fiscal Year 2014 audit determined that some of OPM's regular system vulnerability scans "were not working correctly because the tools did not have the proper credentials, and that some servers were not scanned at all." Id. Another

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

system security tool "was receiving data from only eighty percent of OPM's major IT systems." Id.

45. In his June 16, 2015 written statement, Mr. Esser noted that his office had determined that OPM "does not maintain an accurate centralized inventory of all servers and data bases that reside within the network. Even if the tools I just referenced were being used appropriately, OPM cannot fully defend its network without a comprehensive list of assets that need to be protected and monitored." Id. at 4-5. An agency is required to develop and maintain an inventory of its information systems and audit all activities associated with those information system configurations. See NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (Apr. 30, 2014).

46. In his June 16, 2015 written statement, Mr. Esser stated that, despite Office of Management and Budget requirements, "none of the agency's major applications require [personal identity verification] authentication. Full implementation of PIV verification would go a long way in protecting an agency from security breaches, as an attacker would need to compromise more than a username and password to gain unauthorized access to a system. Consequently, we believe that PIV authentication for all systems should be a top priority by OPM." Esser Statement at 5.

47. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Director Archuleta confirmed that Social Security numbers of individuals affected by the breaches were not encrypted by answering the following question from Rep. Lynch:

> Q: So were the Social Security numbers – were they Encrypted, yes or no?
>
> A: No, they were not encrypted.

OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 14 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management), available at www.fednews.com.

48. During her June 16, 2015 testimony, Director Archuleta confirmed that compromised data was not encrypted by answering the following questions from Rep. Walker:

> Q: Ms. Archuleta, it appears that OPM did not follow the very basic cybersecurity best practices, specifically such as network segmentation and encryption of sensitive data. Should the data have been encrypted? Can you address that?
>
> A: (OFF-MIKE) that the data was not encrypted. And as Dr. Ozment has indicated, encryption may not have been a valuable tool, and in this particular breach. As I said earlier, we are working closely to determine what sorts of additional tools we can put into our system to prevent further . . .
>
> (CROSSTALK)
>
> Q: To use your word you said may not have been. But that didn't answer the question should it have been encrypted? And could that have been another line of defense?
>
> A: I would turn to my colleagues from DHS to determine the use of encryption. But I will say that it was not encrypted at the time of the breach.

Id. at 28.

49. In a June 23, 2015 written statement submitted to the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Mr. Esser again discussed his office's findings, including another discussion of the issues of "Information Security Governance," "Security Assessment and Authorization," and "Technical Security Controls." IT Spending and Data Security at OPM: Hearing Before the Subcommittee on Financial Servs. and General Gov't, Senate Comm. on Appropriations, 114th Cong. (2015) (statement of Michael Esser, Asst. Inspector General for Audits, Office of Personnel Management), available at www.appropriations.senate.gov.

50. In his June 23, 2015 written statement, Mr. Esser stated, "[a]lthough OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today." Id. at 1.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

51. During his June 23, 2015 testimony before the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Richard Spires, Former Chief Information Officer of the U.S. Department of Homeland Security and Internal Revenue Service, and current CEO of Resilient Network Systems, Inc. offered his expert opinion that OPM's deficient security practices could be expected to have resulted in the breaches when he answered the following question from Senator Moran:

> Q : . . . let me first start with a – with a broader question. Based on your understanding of the facts involved here and your best judgement, was the –was the breaches that have occurred at OPM, were they predictable based upon what we knew, looking at the – for example the OIG report. If you saw those reports, is this an outcome that could be expected.
>
> A: I think it is an outcome that could be expected, sir.

Id. at 15 (testimony of Richard Spires, Former Chief Information Officer, U.S. Department of Homeland Security and Internal Revenue Service), available at fednews.com.

52. During his June 24, 2015 testimony before the House Committee on Oversight and Government Reform, OPM Inspector General Patrick McFarland offered his expert opinion that OPM's deficient security practices exacerbated the possibility of the breaches when he answered the following question from Rep. Lynch:

> Q: OK. And the former chief technology officer at the IRS and the Department of Homeland Security said that the breaches were bound to happen given OPM's failure to update its cybersecurity. Is that – is that your assessment, Mr. McFarland?
>
> A: Well, I think without question it exacerbated the possibility, yes.

OPM Data Breach: Part II: Hearing Before the House Comm. on Oversight and Gov't Reform, 114th Cong. 30 (2015) (testimony of Patrick McFarland, Inspector General, Office of Personnel Management), available at www.cq.com.

53. By the conduct described in Paragraphs 32-52, the Defendant has shown a reckless indifference to her obligation to protect the personal information of current and former federal employees, including NTEU's members, from unauthorized disclosure.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

NTEU Members Have Been Injured by Defendant's Failure to Protect Their Personal Information

54. An as yet unknown number of NTEU members have been identified by OPM as having been affected by the breaches described in Paragraphs 10-15 and have been sent the notification described in Paragraphs 10 and 13.

55. Upon information and belief, an as yet unknown number of NTEU members submitted, as part of a background investigation, current or previous versions of SF-86 that resided in an OPM data system at the time of the unauthorized data access and taking announced by OPM on June 12, 2015.

56. Upon information and belief, personal information gathered by investigators (from interviews and other sources) as part of investigations of NTEU members who submitted a SF-86 resided in an OPM data system at the time of the breach announced by OPM on June 12, 2015.

57. Upon information and belief, the personal information described in Paragraphs 55 and 56 has been subject to unauthorized access and taking.

58. Because OPM has stated that the breach announced on June 12, 2015, contained information about background investigations, upon information and belief, it included personal information from SF-85 and SF-85P submitted by NTEU members on the current or previous versions of those forms.

59. Upon information and belief, personal information gathered by investigators (from interviews and other sources) as part of the investigation of NTEU members who submitted SF-85 and SF-85P resided in an OPM data system at the time of the breach announced on June 12, 2015.

60. Upon information and belief, the personal information described in Paragraphs 58 and 59 was subject to unauthorized access and taking.

61. NTEU members submitted the personal information residing in the breached OPM data bases with reason to believe, based on assurances from the government, that the information would be safeguarded from unauthorized disclosure.

62. The current version of the SF-85 contains the following statement on the second page:

> Disclosure of Information
>
> The information you give us is for the purpose of determining your suitability for Federal employment; we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act.

63. The current version of the SF-85P contains the following statement on the second page:

> Disclosure of Information
>
> The information you give us is for the purpose of investigating you for a position; we will protect it from unauthorized disclosure. The collection, maintenance and disclosure of background investigative information is governed by the Privacy Act.

64. The current version of the SF-86 contains the following statement on the second page:

> Disclosure of Information
>
> The information you provide is for the purpose of investigating you for a national security position, and the information will be protected from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information are governed by the Privacy Act.

65. Upon information and belief, previous versions of the SF-85, SF-85P, and SF-86 contained statements similar in content to those set forth in Paragraphs 62-64.

66. Plaintiffs Howell and Ortino were notified by OPM that they were affected by the data breach announced on June 4, 2015.

67. Plaintiffs Howell and Ortino have personal information stored on OPM's information systems and, as part of background investigations related to federal employment,

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

have submitted an SF-85, SF-85P, or SF-86 to OPM.

68. NTEU represents thousands of members who have been notified by OPM that they were affected by the data breach announced on June 4, 2015.

69. NTEU represents thousands of members who have personal information stored on OPM's information systems and who have, as part of background investigations related to federal employment, submitted an SF-85, SF-85P, or SF-86 to OPM.

70. The Defendant showed reckless indifference to her obligation to protect personal information provided by NTEU members with the assurance that the information would be safeguarded.

71. The Defendant's reckless indifference to her obligations has deprived NTEU members of the security that comes from knowing that personal information entrusted to the care of the Defendant will be safeguarded and will not fall into the hands of third parties lacking a legitimate need for the information.

72. The Defendant's reckless indifference to her obligations has already caused NTEU members to lose that sense of security, which can only be restored through relief from this Court.

73. Plaintiffs Howell and Ortino and other NTEU members have reason to believe that, given the two recently announced data breaches and OPM's continued inadequate security measures, the personal information that they have entrusted to the Defendant is at imminent risk of further unauthorized access and that the risk will not be abated until OPM is ordered to correct the security deficiencies discussed above. Each unauthorized access to the personal information that they have entrusted to OPM further violates their constitutional right to informational privacy. The high probability of another unauthorized access of this personal information is further evidenced by Defendant's announcement on June 29, 2015 that a system vulnerability exists with the e-QIP system primarily used by OPM, agencies, and individuals to handle background investigation forms. As a result of this newly-discovered vulnerability, the Defendant has now suspended the entire e-QIP system.

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

74. The Defendant's reckless indifference to her obligations has put NTEU members and their families, friends, and other associates at risk of identity theft, thereby subjecting them to financial peril and inconvenience.

75. The Defendant's reckless indifference to her obligations has put NTEU members and their families, friends, and other associates at risk of harassment, intimidation, or coercion.

76. The Defendant's reckless indifference to her obligations has caused NTEU members emotional distress and anxiety over the effect that these data breaches will have on them, their families, friends, and other associates.

CAUSE OF ACTION

77. Plaintiffs reassert the allegations contained in paragraphs 1 through 76 of this complaint as though contained herein.

78. The Defendant has a duty to safeguard NTEU members' personal information. NTEU members submitted much of the information at issue in this complaint during background investigations required for appointment to, or retention in, their Federal positions. To get, or keep, their jobs, NTEU members had no choice but to divulge information which they would otherwise prefer be kept confidential. This sensitive information was disclosed to the Federal employer, and stored in the Defendant's data systems, with the express assurance that it would be protected from unauthorized disclosure.

79. By failing to heed the repeated warnings of OPM's OIG and otherwise failing to satisfy obligations imposed on her by statute and other appropriate authority, the Defendant has manifested reckless indifference to her obligation to safeguard personal information provided by NTEU members with the assurance that it would be protected against unauthorized disclosure.

80. The Defendant has violated NTEU members' constitutional right to informational privacy, including their right to Due Process under the Fifth Amendment to the U.S. Constitution.

///

///

///

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174

REQUEST FOR RELIEF

WHEREFORE, based on the foregoing, the Plaintiffs request judgment against the Defendant:

A. Declaring that the Defendant's failure to protect NTEU members' personal information was unconstitutional;

B. Ordering the Defendant to provide lifetime credit monitoring and identity theft protection to NTEU members, at no cost to those NTEU members;

C. Ordering the Defendant to take immediately all necessary and appropriate steps to correct deficiencies in OPM's IT security program so that NTEU members' personal information will be protected from unauthorized disclosure;

D. Enjoining the Defendant from collecting or requiring the submission of NTEU members' personal information in an electronic form or storing any such information in an electronic form until the Court is satisfied that all necessary and appropriate steps to safeguard NTEU members' personal information have been implemented;

E. Awarding Plaintiffs their reasonable attorney fees and costs incurred;

F. Ordering such further relief as the Court may deem just and appropriate.

Respectfully submitted,

LEONARD CARDER LLP

DATED: July 7, 2015 By: /s/
Philip C. Monrad
Jennifer Keating

NATIONAL TREASURY EMPLOYEES UNION

DATED: July 7, 2015 By:
Gregory O'Duden
Larry J. Adkins
Paras N. Shah
Allison C. Giles
(pro hac vice applications pending)

Attorneys for Plaintiffs

FILER'S ATTESTATION PURSUANT TO LOCAL RULE 5-1(i)(3)

I, Philip C. Monrad, attest that concurrence in the filing of this document has been obtained from the signatories Jennifer Keating, Gregory O'Duden, Larry J. Adkins, Paras N. Shah, and Allison C. Giles.

Dated: July 7, 2015

LEONARD CARDER, LLP

By: /s/
Philip C. Monrad

LEONARD CARDER, LLP
ATTORNEYS
1330 BROADWAY, SUITE 1450
OAKLAND, CALIFORNIA 94612
TEL: (510) 272-0169 FAX: (510) 272-0174