IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: *NTEU v. Cobert*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	**AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

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, which resulted in unauthorized access to the personal information of 4.2 million 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 experienced another breach, which it later confirmed implicated the personal information of 21.5 million individuals. This breach resulted in unauthorized access to data systems containing materials related to the background investigations of current, former, and prospective federal employees. OPM notified thousands of NTEU members that their personal information was compromised by this data breach.

Among the materials compromised in the breach announced on June 12, 2015, 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 the breach announced on June 12, 2015 involved background investigation materials, 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, 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.

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

2. This lawsuit was originally filed in the Northern District of California before being transferred for coordinated or consolidated pretrial proceedings to this District. Plaintiffs have not waived—and, by the filing of this amended complaint, do not waive—their rights under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C. § 1407(a), to seek a remand to the Northern District of California at the conclusion of pretrial proceedings. Thus, Plaintiffs, here, allege that venue is proper in the Northern District of California and also proper in this District.

3. Venue is proper in the Northern District of California 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 Stephen Howell and Jonathon Ortino reside within the Division; and Plaintiff Ortino works within the Division. Thus, Plaintiffs Howell and Ortino's respective injuries have occurred, at least in substantial part, within the Division.

4. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(e) because Defendant, Beth Cobert, Acting Director of the Office of Personnel Management, in her official capacity, resides in the District of Columbia.

PARTIES

5. Plaintiff 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.

6. Plaintiff Eugene Gambardella resides in Manalapan, NJ. He is employed by Customs and Border Protection (CBP) in Newark, NJ, as a Senior Import Specialist. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU. Mr. Gambardella submitted an SF-85P when he was hired by CBP, and later submitted an SF-86 to CBP during a standard reinvestigation. Through these forms, he disclosed or authorized the release to OPM of, among other information, medical information (including mental health information), financial information (including his investment accounts), marital information, nonpublic information about his family

(including the citizenship papers, immigration numbers, and passport numbers of relatives), and his Social Security Number.

7. 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. Mr. Howell submitted an SF-86 when he was hired by IRS, disclosing or authorizing the release to OPM of, among other information, medical information (including mental health information), marital information, nonpublic information about his family, and his Social Security Number.

8. Plaintiff Jonathon Ortino resides in Burlingame, CA (San Mateo County). He is employed by CBP 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. Mr. Ortino submitted an SF-86 when he was hired by CBP, disclosing or authorizing the release to OPM of, among other information, medical information (including mental health information), financial information, marital information, nonpublic information about his family, and his Social Security Number. Mr. Ortino was subject to a periodic reinvestigation in 2012.

9. Defendant Beth F. Cobert is Acting Director of OPM. Acting Director Cobert succeeded former Director of OPM Katherine Archuleta, who resigned as Director in the wake of the data breaches described in this amended complaint. As

Acting Director, Ms. Cobert is responsible for executing, administering, and enforcing civil service laws and regulations, including the requirement that federal government applicants and employees undergo background investigations. She is also responsible for ensuring that personal information entrusted to OPM is protected from unauthorized disclosure. The Acting Director is sued solely in her official capacity.

STATEMENT OF CLAIMS

OPM's Data Collection and Retention

10. 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.

11. 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.

12. 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 Breach Announced on June 4, 2015

13. OPM experienced a cybersecurity incident, which it announced on June 4, 2015, that compromised the personal information of 4.2 million individuals. OPM sent letters to those affected by the incident to notify them that their personal information was compromised.

14. OPM first detected the incident in April 2015. See News Release, OPM to Notify Employees of Cybersecurity Incident, Office of Personnel Management (June 4, 2015). This cybersecurity incident is believed to have been perpetrated in October 2014. See Sean Lyngaas, Exclusive: The OPM Breach Details That You Haven't Seen, Federal Computer World (Aug. 21, 2015), available at https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx (drawing upon timeline for OPM cybersecurity incidents provided in July 14, 2015 document "prepared by federal investigators for the office of U.S. CIO Tony Scott"). During

this time, the perpetrators of the cybersecurity incident accessed and took personal information housed in the accessed OPM data systems, as detailed below.

15. 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.

16. Thousands of NTEU members were determined by OPM to have been affected by this first data breach and have received the notification described in Paragraphs 13 and 15. Those NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, were subject to unauthorized access of their personal information through the breach, and the taking of that information.

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

The Breach Announced on June 12, 2015

18. On June 12, 2015, OPM announced a second data breach. OPM first detected the incident in May 2015. See News Release, OPM Announces Steps to

Protect Federal Workers and Others From Cyber Threats, Office of Personnel Management (July 9, 2015). This data breach is believed to have been perpetrated in July and August 2014. See Sean Lyngaas, Exclusive: The OPM Breach Details That You Haven't Seen, Federal Computer World (Aug. 21, 2015), available at, https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx (referencing timeline for OPM cyber incidents provided in July 14, 2015, document "prepared by federal investigators for the office of U.S. CIO Tony Scott"). During this time, the perpetrators of the data breach accessed and took personal information housed in the accessed OPM data systems, as detailed below.

19. Based on OPM's public announcements, this data breach involved OPM systems, such as those discussed in Paragraph 12, containing, among other information, information related to the background investigations of current, former, and prospective federal government employees. In all, this breach compromised the personal information of 21.5 million individuals. OPM would later announce, on September 23, 2015, that the perpetrators of the breach accessed and took the fingerprints of approximately 5.6 million current, former, and prospective federal government employees. OPM has sent letters to those affected by this breach. NTEU members who underwent federal background investigations were subject to unauthorized access of their background investigation information through the breach, and the taking of that information.

20. As part of the background investigations described in Paragraph 11, 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).

21. 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 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.

22. 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."

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

24. 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.

25. 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.

26. 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.
>
> What is the prognosis?

27. 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.

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

29. 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.

30. The current version of the SF-86 includes an "Authorization for Release of Information" similar in content to authorization described in Paragraph 25 for the SF-85P.

31. 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 26 for the SF-85P.

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

33. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, then-Director of OPM, Katherine 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).

34. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Donna Seymour, then-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).

35. 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.

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

36. 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.

37. 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, such as executive orders on cybersecurity and standards promulgated by the National Institute of Standards and Technology (NIST), 44 U.S.C. § 3554(a)(1)(B).

38. 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.

39. 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).

40. Director Archuleta repeated the assertions described in Paragraph 39 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 Gov't, Senate Comm. on Appropriations, 114th Cong. 4-5 (2015) (statement of Katherine Archuleta, Director, Office of Personnel Management).

41. In its audit report for Fiscal Year 2014, required by FISMA, OPM's Office of the Inspector General (OPM OIG) 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).

42. 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").

43. 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.

44. 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.

45. 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.

46. 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.

47. 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.

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

49. 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).

50. In his June 16, 2015 written statement, Mr. Esser stated that, despite OMB 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.

51. 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).

52. 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.

53. 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.

54. 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.

55. 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).

56. 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.

57. In a recent media interview Clifton Triplett, OPM's senior cybersecurity advisor, reflecting back on the breaches and the "emergency IT security upgrades" required in their wake, conceded, "[w]e're a wonder poster child of how bad it can be if you don't do the right thing." Jack Moore, OPM: A Year After the Big Breach, Nextgov.com (May 11, 2016), available at, www.nextgov.com/cybersecurity/2016/05/opm-year-after-big-breach/128233.

58. By the conduct described in Paragraphs 36-57, 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—such as Plaintiffs Gambardella, Howell, and Ortino—from unauthorized disclosure.

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

59. An unknown number of NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, have been identified by OPM as having been affected by the breaches described in Paragraphs 13-19 and have been sent the notifications described in Paragraphs 13 and 15.

60. An unknown number of NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, 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.

61. Personal information gathered by investigators (from interviews and other sources) as part of investigations of NTEU members who submitted a SF-86, including Plaintiffs Gambardella, Howell, and Ortino, resided in an OPM data system at the time of the breach announced by OPM on June 12, 2015.

62. The personal information described in Paragraphs 60 and 61 has been subject to unauthorized access and taking by those who perpetrated the breach announced on June 12, 2015.

63. An unknown number of NTEU members, including Plaintiff Gambardella, submitted, as part of a background investigation, current or previous versions of SF-85 or SF-85P that resided in an OPM data system at the time of the unauthorized data access and taking announced by OPM on June 12, 2015.

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

65. Upon information and belief, the personal information described in Paragraphs 63 and 64 was subject to unauthorized access and taking by those who perpetrated the breach announced on June 12, 2015.

66. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, submitted the types of inherently personal information described in Paragraphs 21-32 to OPM and that information resided on the breached OPM databases. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino submitted that inherently personal information with reason to believe, based on assurances from the government, that the information would be safeguarded from unauthorized disclosure.

67. 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.

68. 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.

69. 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.

70. 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 67-69.

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

72. Plaintiffs Gambardella and Howell were notified by OPM that they were affected by the data breach announced on June 12, 2015. Each has inherently personal information that resided and continues to reside on OPM's information systems as part of his or her background investigation(s) related to federal employment.

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

74. NTEU likewise represents thousands of other members who have personal information stored on OPM's information systems and who have been notified by OPM that they were affected by the data breach announced on June 12,

2015, and who have, as part of background investigations related to federal employment, submitted an SF-85, SF-85P, or SF-86 to OPM.

75. The Defendant showed reckless indifference to her obligation to protect personal information provided by NTEU members—including Plaintiffs Gambardella, Howell, and Ortino—with the assurance that the information would be safeguarded.

76. The harm to NTEU members, including Plaintiffs Gambardella, Howell, and Ortino occurred the moment that their inherently personal information—which they provided to OPM on the promise of confidentiality and as a condition of their federal employment—was taken by unauthorized intruders from OPM's databases. This constitutionally protected private information should have been properly protected from unauthorized access and taking by OPM, but was not, as described above.

77. The Defendant's reckless indifference to her obligations has deprived NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, of the security that comes from knowing that the inherently personal information that they provided to the Defendant on the promise of confidentiality will be safeguarded and will not fall into the hands of third parties lacking authorization to view the information.

78. The Defendant's reckless indifference to her obligations has caused NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, to lose that sense of security, which can only be restored through relief from this Court.

79. In or around February 2016, Plaintiff Gambardella attempted to electronically file a joint federal tax return for tax year 2015. He was unable to do so because, as the IRS notified him, an individual federal tax return had already been filed in his name for 2015. That individual federal tax return was fraudulently filed in Mr. Gambardella's name.

80. After learning of the fraudulently-filed return, Mr. Gambardella expended time and resources interfacing with IRS to deal with the issue of the already-filed fraudulent return. He then had to re-file his 2015 federal return. Due to the prior fraudulent filing, however, Mr. Gambardella could not file electronically, but had to file in paper form. He was unable to file until the end of February 2016. The paper federal return, which takes longer to process than an electronically filed return, was not processed by IRS until April 6, 2016.

81. Mr. Gambardella believes he is entitled to a federal tax refund of approximately $7,000. However, as of the filing of this amended complaint, Mr. Gambardella still has not received his federal tax refund.

82. Apart from the OPM data breaches announced in June 2015, Mr. Gambardella has not, to the best of his knowledge, had his personal information exposed in any other public or private sector data breach. Nor has he, to the best of his knowledge, ever been the victim of identity theft other than the instances described in this amended complaint.

83. Because the data breaches announced in June 2015 are the only data breaches that have implicated his personal information, Mr. Gambardella

reasonably believes that the fraudulent federal tax return, which has led to a delay in his approximately $7000 federal tax refund, stems from the OPM data breaches. This delay has led to a loss of use of the refund money and a loss of interest on that money.

84. Mr. Gambardella has experienced other harm that he reasonably believes, given that he has not been affected by any other breaches, is attributable to the breaches announced in June 2015. Earlier this year, he had three separate fraudulent charges appear on an existing credit card. Each was for an amount over $300. He was able to have those fraudulent charges resolved after contacting his credit card company.

85. Apart from the OPM data breaches announced in June 2015, Plaintiff Howell has not had, to the best of his knowledge, his personal information exposed in any other public or private sector data breach.

86. Apart from the OPM data breaches announced in June 2015, Plaintiff Ortino has not had, to the best of his knowledge, his personal information exposed in any other public or private sector data breach.

87. Plaintiffs Gambardella, Howell, and Ortino, and other NTEU members who were notified that they were implicated by one or both of the breaches announced in June 2015, have reason to believe that, given the June 2015 breaches and OPM's continued inadequate security measures, the personal information that they have entrusted to the Defendant on the promise of confidentiality is at substantial risk of further unauthorized access. They reasonably believe 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.

88. The substantial risk of another unauthorized access of this personal information is further evidenced by OPM OIG's Final Audit Report for Fiscal Year 2015, issued on November 10, 2015. In that report, the OIG explained that "for many years, we have reported critical weaknesses in OPM's ability to manage its IT environment, and warned that he agency was at an increased risk of a data breach." Report at 5. Yet, "OPM continuously failed a variety of FISMA metrics and carried material weaknesses in the annual FISMA reports." Id. Indeed, the OIG concluded, "[o]ur recommendations appeared to garner little attention, as the same findings were repeated year after year." Id. The OIG added that in light of "the overall lack of compliance that seems to permeate the agency's IT security program," "we are very concerned that the agency's systems will not be protected against another attack." Id.

89. In the same fiscal year 2015 audit report, the OIG noted that of particular concern was OPM's continued "inability to accurately inventory its systems and network devices," which "drastically diminishes the effectiveness of its security controls." Id. at 6. While, in the wake of the data breaches announced in June 2015, "OPM has implemented a large number of improved security monitoring tools," "without a complete understanding of its network, it cannot adequately

monitor its environment and therefore the usefulness of these tools is reduced." Id. "This same concern extends to OPM's vulnerability scanning program." Id.

90. Further demonstrating the substantial risk of another unauthorized access of the personal information of Plaintiffs Gambardella, Howell, and Ortino and other NTEU members is OPM's flawed effort to secure an able contractor to overhaul its information technology security. In July 2015, OPM awarded a sole source control award to Imperatis, formerly known as Jorge Scientific Corporation, to overhaul OPM's IT infrastructure. Senator Claire McCaskill wrote to then-Director Archuleta expressing concern about its decision to "rush the award, and its decision to not engage in a full and open competition." See Letter from Hon. Claire McCaskill to Hon. Beth Cobert dated May 13, 2016 (reiterating previously aired concerns). She was particularly concerned about the "history of misbehavior of the company's employees." Id. In light of the company's "troubled history with government contracting," Senator McCaskill was "not entirely surprised" when her office was informed on May 10 that Imperatis "had abruptly ceased operations" on its contract with OPM. Id. Indeed, on May 9, Imperatis "stopped coming to work," causing OPM to terminate the company's contract that same day," even though Imperatis "had about a month of work left under the deal." Jason Miller, Vendor Hired to Improve Security of OPM's Network Goes Out of Business, federalnewsradio.com (May 16, 2016) (noting that "Imperatis referenced financial distress at the company as the reason for the immediate closure"). The status of

Imperatis's now abandoned effort to overhaul OPM's information technology infrastructure is unknown.

91. OPM's OIG continues to express concern over OPM's plan to upgrade its information technology security, further highlighting the substantial risk of another unauthorized access of the personal information of Plaintiffs Gambardella, Howell, and Ortino and other NTEU members. OPM's OIG, in an interim status report issued on May 18, 2016, expressed continued concern about OPM's efforts to upgrade its information technology security and, in particular, its failure to properly develop a proper project plan for the upgrade in accordance with OMB requirements. As OPM's OIG noted, nearly a year ago, it "expressed the opinion that OPM's desire to better secure its IT environment as quickly as possible, [which led to its] declining to perform many of the mandatory planning steps [required for such a project by OMB], resulted in a high risk that the Project would fail to meet its objectives." Report at 3. That risk, OPM's OIG reports, has only grown. As it stated, "[n]ow that we have reviewed OPM's recent Business Case and its support activities in depth, we are even more concerned about the lack of disciplined capital planning processes." Id. at 3-4 (noting that "OPM did not develop a realistic budget based on an understanding of the number of systems that would need to be migrated to the new [information technology] environment, the level of effort associated with the required modernization and security updates, and the cost of this process").

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

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

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

CAUSE OF ACTION

95. Plaintiffs reassert the allegations contained in paragraphs 1 through 94 of this complaint as though contained herein.

96. The Defendant has a duty to safeguard NTEU members' personal information. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, 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, including Plaintiffs Gambardella, Howell, and Ortino, 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.

97. 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, including Plaintiffs Gambardella, Howell, and Ortino, with the assurance that it would be protected against unauthorized disclosure.

98. The Defendant has violated Plaintiffs Gambardella, Howell, and Ortino's constitutional right to informational privacy, including their right to due process under the Fifth Amendment to the U.S. Constitution. The Defendant has likewise violated the constitutional right of informational privacy of all other NTEU members whose personal information was exposed by the breaches announced on June 4, 2015 and June 12, 2015.

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,

Gregory O'Duden
Larry J. Adkins

/s/ Paras N. Shah

Paras N. Shah
Allison C. Giles
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

Attorneys for Plaintiffs

Of Counsel:

Leon O. Dayan
Devki K. Virk
BREDHOFF & KAISER PLLC
805 15th Street N.W.
Suite 1000
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: ldayan@bredhoff.com
Email: dvirk@bredhoff.com

Attorneys for Plaintiffs

June 3, 2016

CERTIFICATE OF SERVICE

I hereby certify that on June 3, 2016, I filed the above amended complaint with the Court's CM/ECF system, which will send notice to the other parties.

/s/ Paras N. Shah
Paras N. Shah