IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DENISE NEMETH-GREENLEAF,

JASON JUDKINS,

JON MICHEL,

DONNA NEMETH, and

MICHAEL RIFER, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
1900 E. Street, NW
Washington, DC 20415,

CHARLES EZELL, Acting Director of U.S. Office of Personnel Management, in his official capacity,

AMANDA SCALES, U.S. Office of Personnel Management Chief of Staff, in her official capacity,

BRIAN BJELDE, U.S. Office of Personnel Management Senior Advisor, in his official capacity,

GREGORY BARBACCIA, U.S. Federal Chief Information Officer, in his official capacity,

UNITED STATES DEPARTMENT OF THE TREASURY,
1500 Pennsylvania Ave NW
Washington, DC 20500,

SCOTT BESSENT, Secretary of the U.S. Department of the Treasury, in his official capacity,

Defendants.

Case No.

CLASS ACTION COMPLAINT

(JURY TRIAL DEMANDED)

CLASS ACTION COMPLAINT

Plaintiffs Denise Nemeth-Greenleaf, Jason Judkins, Jon Michel, Donna Nemeth, and Michael Rifer,[1] on behalf of themselves and all persons similarly situated, allege the following:

I. INTRODUCTION

1. A government contractor called the subject of this lawsuit—the unauthorized access of millions of federal employees' personal information—"the largest data breach and the largest IT security breach in our country's history."[2] Defendants' failure to protect government employees' privacy is the biggest breach of American trust by political actors since Watergate. Plaintiffs bring this lawsuit to protect their privacy and uphold the rule of law.

2. Plaintiffs Denise Nemeth-Greenleaf, Jason Judkins, Jon Michel, Donna Nemeth, and Michael Rifer, individually and on behalf of the proposed class described below, bring this action for injunctive relief, actual damages and statutory damages against Defendant United States Office of Personnel Management ("OPM"), Defendant Charles Ezell, Defendant Amanda Scales, Defendant Brian Bjelde, Defendant Gregory Barbaccia, Defendant United States Department of the Treasury ("Treasury Department"), and Defendant Scott Bessent (collectively, "Defendants"), for Defendants' unlawful ongoing, systemic, and continuous disclosure of personal, health, and financial information—including personally identifiable information including employees' full name, address, Social Security Number, driver's license, or U.S. Passport Number ("PII"), personal health information including disability status, health insurance provider information, and other medical records ("PHI"), and personal financial information including payroll, direct deposit, and financial account numbers ("PFI"), (collectively, "Personal Sensitive Information" or

[1] Pursuant to Local Civil Rule 5.1(c)(1), a notice containing the required information for each Plaintiff will be filed simultaneously under seal.

[2] Charlie Warzel and Ian Bogost, THE ATLANTIC, "The Government's Computing Experts Say They Are Terrified," (Feb. 7, 2025), https://perma.cc/6XFF-75N6.

"PSI")—contained in Defendants' records to non-governmental employee and private citizen Elon Musk, as well as other non-governmental employee members of the "task force" associated with the so-called "Department of Government Efficiency" ("DOGE"), and to any other unauthorized person.

3. Millions of federal employees entrust their PSI to the federal government as a condition of their employment, with the expectation that this data will be securely maintained. This data is collected and maintained by various governmental agencies, all of whom have a statutory duty pursuant to the Privacy Act of 1974 ("Privacy Act") to protect that information from improper disclosure and misuse.

4. Since the 2025 inauguration of President Donald J. Trump, Defendants OPM and Treasury Department have not only failed to safeguard that data but have in fact willfully and intentionally permitted it to be accessed by individuals outside the United States government without legal justification and in violation of the Privacy Act. The individuals granted access to the PSI are, essentially, hackers who have been given access to the data by the government itself. They are individuals who lack authorization to access such information; they are non-government employees who do not have proper security clearances and are uninhibited by the restrictions required by law and placed on federal government employees. Such access is a breach of the privacy rights afforded to federal employees as well as those afforded to American citizens in general. These unlawful disclosures already have—and will continue to have—deleterious adverse effects on federal workers that have caused them harm, including but not limited to actual damages, ongoing vulnerability to further hacking, cyber-attacks, fraudulent activity, actual theft, and ongoing mental distress.

II. JURISDICTION AND VENUE

5. Pursuant to the Class Action Fairness Act, this Court has original jurisdiction because the aggregate claims of the putative Class Members exceed $5 million, exclusive of interest and costs, and at least one Plaintiff brings class claims on behalf of citizens of states different than Defendants' states of citizenship. 28 U.S.C. §§ 1332(d)(2) and (6).

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

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

8. This Court has personal jurisdiction over Defendants OPM and the Treasury Department because they maintain headquarters in the District of Columbia and the relevant conduct occurred in the District of Columbia.

9. This Court has personal jurisdiction over Defendants Ezell, Scales, Barbaccia, Bjelde, and Bessent because they work as OPM Director, Chief of Staff, Chief Information Officer ("CIO"), Senior Director, and Treasury Department Director, respectively, in the District of Columbia offices, and the relevant conduct occurred in the District of Columbia.

10. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants OPM and Treasury Department are located in the District of Columbia and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in the District of Columbia.

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

III. PARTIES

12. Defendant OPM is a U.S. agency with headquarters at 1900 E. Street, NW, Washington, DC 20415. Defendant OPM is responsible for, among other things, managing the

civil service of the federal government, recruitment of new government employees, and managing their health insurance and retirement benefits program.

13. Defendant Ezell is the Acting Director of OPM and works at the agency headquarters in Washington, D.C. Plaintiffs bring this action against Ezell in his official capacity as Director of the OPM only.

14. Defendant Scales is the OPM Chief of Staff and works at the agency headquarters in Washington, D.C. She assists Defendant Ezell in overseeing a broad range of policy and administrative issues in the OPM, including oversight of its cybersecurity policies and practices. Defendant Scales is a former private employee of Elon Musk and, upon information and belief, is acting upon Mr. Musk's orders. Plaintiffs bring this action against Scales in her official capacity as OPM Chief of Staff only.

15. Defendant Bjelde is a Senior Advisor at OPM and works at the agency headquarters in Washington, D.C. He assists Defendant Ezell in overseeing a broad range of policy and administrative issues in the OPM, including oversight of its cybersecurity policies and practices. Defendant Bjelde is a former employee of Elon Musk and, upon information and belief, is acting upon Mr. Musk's orders. Plaintiffs bring this action against Bjelde in his official capacity as OPM Senior Advisor only.

16. Defendant Barbaccia is the CIO for OPM and works at the agency headquarters in Washington D.C. He oversees OPM's software systems and cybersecurity policies and practices. Plaintiffs bring this action against Barbaccia in his official capacity as CIO for OPM only. Defendants Ezell, Scales, Barbaccia, Bjelde, and OPM are referred to as the "OPM Defendants" collectively.

17. Defendant United States Department of Treasury is a federal agency with headquarters at 1500 Pennsylvania Ave., NW, Washington, DC 20220. The Treasury Department is responsible for, among other things, the Bureau of the Fiscal Service, which distributes trillions of dollars in payments each year, including payments for federal employees' salaries.

18. Defendant Bessent is the Secretary of the Treasury Department and works at the agency headquarters in Washington, D.C. Plaintiffs bring this action against Bessent in his official capacity as Director of the Treasury Department only. Defendants Bessent and Treasury Department are referred to as "Treasury Department Defendants" collectively.

19. Plaintiff Denise Nemeth-Greenleaf is a resident of the State of Maine. She is currently employed with the Department of the Navy, at Portsmouth Naval Shipyard in Kittery, Maine, where she is an Industrial Program Specialist. Plaintiff Nemeth-Greenleaf learned about Defendants' breaches of her PSI from media reports. In response, Plaintiff Nemeth-Greenleaf purchased identity theft protection service from Aura.

20. Plaintiff Jason Judkins is a resident of the Commonwealth of Massachusetts. He is currently employed with the Bureau of Prisons at Federal Medical Center, Devens. Plaintiff Judkins learned about the Defendants' breaches of his PSI from media reports. In response, Plaintiff Judkins purchased credit and identity theft monitoring through Aura Identity Protection.

21. Plaintiff Jon Michel is a resident of the State of Indiana. He is currently employed with the United States Army Corp of Engineers at Cannelton Locks and Dam, where he works as a Lock Operator. Plaintiff Michel learned about Defendants' breaches of his PSI from media reports. In response, Plaintiff Michel purchased credit and identity theft monitoring through Lifelock by Norton.

22. Plaintiff Donna Nemeth is a resident of the State of Colorado. She is currently employed with the United States Department of Agriculture, Forest Service, at the Rocky Mountain Regional Office, where she works as the Agency's Press Officer. Plaintiff Nemeth learned about Defendants' breaches of her PSI from media reports. In response, Plaintiff Nemeth purchased identity theft protection service from Aura.

23. Plaintiff Michael Rifer is a resident of Washington, D.C. He is currently employed with the United States Agency for International Development ("USAID"), as the Managing Director of Relationship Management Systems. Plaintiff Rifer first learned about the Defendants' breaches of his PSI from media reports. In response, Plaintiff Rifer purchased advanced credit and identity theft monitoring through American Express.

IV. FACTUAL BACKGROUND

A. Defendants Treasury Department and OPM Permitted Unlawful Access to Information Protected by the Privacy Act

24. Millions of individuals, including Plaintiffs and proposed Class Members, engage in financial transactions with the federal government. Defendant Treasury Department disburses and collects trillions of dollars to and from the American people, including federal employees.

25. The Bureau of the Fiscal Service effectuates these financial transactions for the Defendant Treasury Department. The Bureau of the Fiscal Service collects and maintains personal data, including certain PSI, on federal employees such as names, Social Security numbers, birth dates, and bank account information, to ensure the secure and timely transfer of funds to federal employees for, among other things, wage compensation and tax purposes.

26. Defendant OPM operates as the federal government's chief human resources agency. In that capacity, Defendant OPM maintains electronic personnel files containing certain PSI, through its "Enterprise Human Resources Integration" ("EHRI") program. As part of the

EHRI program, OPM manages access to the "electronic Official Personnel Folder" ("eOPF") for federal employees across agencies of the Executive Branch, and collects, integrates, and publishes data for approximately 2 million federal employees on a bi-weekly basis.

27. PSI maintained by Defendant OPM includes, among other information, copies of federal employees' birth certificates, documents identifying their Social Security numbers and birth dates, personal biographical information, disability status and health insurance program enrollment information, 401(k) enrollment information, personnel action investigations, character and fitness investigations, and more.

28. Defendant OPM also oversees background checks and security clearance investigations, for which it collects and maintains additional sensitive personal information, including PSI, for federal employees and applicants including passport information, residency details, fingerprints, and records pertaining to employees' psychological and emotional health and finances.

29. Defendant OPM also handles many aspects of the federal employee recruitment process, including managing federal job announcements, conducting background investigations and security clearances, overseeing federal merit systems, managing personal retirement and health benefits, providing training and development programs, and developing government personnel policies. As part of the recruitment process, OPM collects and maintains federal applicants' records including PSI, background investigations, and security clearance forms.

30. Federal laws protect PSI from improper disclosure and misuse, including by barring disclosure to individuals who lack a lawful and legitimate need for it or who lack proper security clearance to access such information. Prior to January 2025, only individuals with a "need to know" (*i.e.,* individuals who are conducting background checks, and suitability determinations,

among others) could access PSI; prior to gaining access, those personnel must have undergone their own security clearance process.

31. Beginning shortly after the inauguration of President Donald Trump on January 20, 2025, Defendants OPM and Treasury Department illegally and improperly violated these restrictions on disclosure of PSI by giving access to that PSI to individuals without a lawful or legitimate need for such data and without their having undergone the security clearance process.

32. The "Department of Governmental Efficiency" or "DOGE" was established by presidential executive order on January 20, 2025, with the stated purpose of downsizing the federal government by abolishing entire federal agencies and terminating massive numbers of federal employees. It is purportedly headed by Elon Musk, the billionaire CEO and founder of Tesla and SpaceX and the owner of X (formerly Twitter). At the time of DOGE's creation and continuing through the beginning of the breach of Plaintiffs' PSI here, Musk was not a federal employee in any capacity. Musk has been accused of implementing anti-worker policies, union-busting, and instituting large employee layoffs without regard for the rights of employees across all his companies. All DOGE associates are individuals who currently, or previously have, worked for Musk at his private companies.

33. In late January, Elon Musk, with the assistance of individuals who were not employees of any federal agency and lacked a lawful or legitimate need for such data, sought access to the records maintained by the Treasury Department and/or the Bureau of the Fiscal Service.

34. Days after being sworn in as Secretary of the Treasury, Defendant Bessent improperly granted DOGE-affiliated individuals full access to the Bureau of the Fiscal Service's data, and the computer systems that house such data, which includes Plaintiffs' PSI. Defendant

Bessent did so without legal justification, and without making any efforts to ensure that disclosures were made consistent with Treasury Department policies. Contrary to policy, Defendants knowingly provided access to PSI maintained by Defendant Treasury Department to individuals who had not obtained security clearance, who had not taken the required annual Cyber Security and Privacy Awareness training courses, and who were not accessing that information for a legitimate purpose such as fraud detection and payment/benefits processing.

35. For example, in or around late January 2025, Defendant Treasury Department gave Marko Elez, a 25-year-old engineer whose limited career includes working for two Elon Musk Companies, direct access to Treasury Department systems responsible for nearly all payments made by the United States, including payments to federal workers such as the Plaintiffs and the proposed Class Members. Mr. Elez was not, at the time, a government employee with the proper security clearance or training to access these data or systems.[3]

36. Likewise, also in late January 2025, employees at OPM were instructed to provide information on federal employees to Defendant Scales, who worked for xAI, a private corporation of which Elon Musk is the Chief Executive Officer. Although Defendant Scales neither had the requisite security clearance to access the data nor was a government employee at that time, she was nevertheless allowed to access and control the massive database holding information on millions of federal employees, including Plaintiffs' PSI.

37. Defendants, including but not limited to Defendant Scales, then improperly granted other DOGE-affiliated individuals, including Elon Musk, full access to OPM's data and the

[3] On February 6, 2025, Elez resigned after the media reported on a number of 2024 posts from an account connected to Elez on Musk's X platform. Those posts included "Normalize Indian hate," and "I just want a eugenic immigration policy, is that too much to ask." *See* Bobby Allyn and Shannon Bond, NPR, "Member of Elon Musk's DOGE team resigns after racist posts resurface," (Feb. 7, 20205), https://perma.cc/F7BF-DZVX.

computer systems that house such data, doing so without legal justification, and without making any efforts to ensure that disclosures were made consistent with OPM's policies.

38. For example, unfettered and unlawful administrative access to PSI maintained by OPM was granted to non-governmental employees Akash Bobba, Edward Coristine, Luke Farritor, Gautier Cole Killian, Gavin Kliger, and Ethan Shaotran. Neither Mr. Musk nor these individuals have proper security clearance to access these data or systems.

39. These individuals have limited work experience, most of which is for Musk-associated companies. Akash Bobba recently graduated from college and previously interned at Meta and Palantir, a technology firm. Edward Coristine is a 2022 high school graduate who served as an intern at Musk's Neuralink and goes by the nickname of "bigballs" on LinkedIn. Luke Farritor is a former intern at Musk's SpaceX who is now listed as an "executive engineer." Gautier Killian attended two years of college after graduating high school and was, as of February 2, 2025, simply listed as a "volunteer" with DOGE. Gavin Kliger most recently worked for the AI company Databricks; his social media posts include one titled "The Curious Case of Matt Gaetz: How the Deep State Destroys Its Enemies." Ethan Shaotran reported in September that he was a senior at Harvard and was a previous runner-up in a hackathon held by xAI, Musk's AI company. Notably, Edward Coristine was fired from a previous data security internship with Path Network after he leaked internal information to competitors.[4]

40. These actions represent "a dramatic shift in the way the government's business has traditionally been conducted."[5] Normally, access to government databases is highly restricted, with strict, differential controls on what a government employee, contractors, and civil-service

[4] Jason Leopold *et al.*, BLOOMBERG, "Musk's DOGE teen was fired by cybersecurity firm for leaking company secrets," (Feb. 7, 2025), https://perma.cc/7N54-FA5F.
[5] Charlie Warzel and Ian Bogost, THE ATLANTIC, "The Government's Computing Experts Say They Are Terrified," (Feb. 7, 2025), https://perma.cc/6XFF-75N6.

government workers may access versus the limited data that a political appointee may access, and with limited visibility into the system as a whole *by design*.[6]

41. Government security protocols are so strict that a contractor plugging a non-government-issued computer into an ethernet port in a government agency office is normally considered a "major security violation."[7] From a security perspective, that Defendants have allowed these individuals access likely without proper security clearances is "madness."[8]

42. That is because even with "read only" access to Plaintiffs' PSI—which Plaintiffs do not concede is the highest level of access Defendants have so far provided to unauthorized users—"Musk's people could easily find individuals in databases or clone entire servers and transfer that secure information somewhere else."[9] And whatever data is siphoned now, including Plaintiffs' PSI, "could be [Musk's] forever."[10]

43. This access is also plainly unlawful.

44. At no point prior to permitting unauthorized individuals access to Plaintiffs' PSI did any of the Defendants seek the written consent of the Plaintiffs or proposed Class Members, as is required by law.

45. Further, it is clear from public reporting that sensitive agency information, including Plaintiffs' PSI, is being used in ways that suggest Defendants' willful, intentional, and flagrant disregard of Plaintiffs' rights and basic security best practices.

46. For example, representatives from Elon Musk's U.S. DOGE Service have fed sensitive data from across the U.S. Department of Education into artificial intelligence software to

---

[6] *See id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

probe the agency's programs and spending.[11] According to two people with knowledge of the DOGE team's actions, "[t]he AI probe includes data with personally identifiable information for people who manage grants, as well as sensitive internal financial data[.]"[12] The DOGE team aims to repeat this process across federal agencies:

> The DOGE team plans to replicate this process across many departments and agencies, accessing the back-end software at different parts of the government and then using AI technology to extract and sift through information about spending on employees and programs, including DEI initiatives, according to another person familiar with the DOGE process, who also spoke on the condition of anonymity because they were not authorized to describe it.[13]

47. In fact, following a lawsuit from 19 state attorney generals against President Donald Trump, and the Treasury Department Defendants, a federal district court judge concluded that there were sufficient grounds for a temporary restraining order to enjoin defendants from granting access to the Treasury payment systems to political appointees, special government employees, and any government employee outside of the Treasury Department. This extraordinary relief was granted because such access increases the risk of "disclosure of sensitive and confidential information and the heightened risk that the [Treasury payment systems] will be more vulnerable to hacking[,]" combined with the likelihood that the States would prevail on the merits on their claims.[14]

48. This unlawful and flagrant intrusion into federal employee's privacy is unprecedented.

---

[11] Hannah Natanson *et al.*, THE WASHINGTON POST, "Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts," (Feb. 6, 2025), https://perma.cc/3JGS-FUHR.
[12] *Id*.
[13] *Id*.
[14] *State of New York et al. v. Donald J. Trump et al.*, 1:25-cv-01144-JAV, ECF No. 6 at 2 (S.D.N.Y.).

B. Plaintiffs and Proposed Class Members Were and Are Harmed Because of Defendants' Violations of the Privacy Act

49. Federal workers such as the Plaintiffs and proposed Class Members cannot avoid having PSI for themselves and their family members maintained in government records and government record-keeping systems.

50. Defendants' actions in granting DOGE-affiliated individuals full, continuous, and ongoing access to that information means that these employees have no assurance that their PSI will receive the protection that federal law affords.

51. Permitting access to protected information puts the PSI for the Plaintiffs and proposed Class Members at real risk, making them vulnerable to fraud, cyber-attack, and actual theft.

52. Permitting access to protected information also puts Plaintiffs, and proposed Class Members, at great personal risk. Indeed, on February 4, 2025, a website called "DEI Watch List" gained national attention. The website included photos, names and other information on federal employees who had worked on Diversity, Equity, and Inclusion ("DEI") initiatives and/or attended DEI trainings. The type of work performed by federal employees, as well as certain trainings they gave or attended, is information maintained by Defendant OPM. Initially, the photos of federal employees were published under the headline "Targets."

53. Due to Defendants' willful, intentional, and flagrant disregard of Plaintiffs' and Class Members' privacy rights, Plaintiffs and Class Members have suffered and will continue to suffer damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress. They have suffered, or are at risk of suffering from:

a) The loss of the opportunity to control how their PSI is used;

b) The compromise, publication, and/or theft of their PSI and the PSI of their family members;

c) Out of pocket costs associated with the prevention, detection, and recovery from identify theft and/or unauthorized use of accounts, including financial and medical accounts;

d) Lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate any consequences from OPM and Treasury breaches, including but not limited to efforts spent researching how to prevent, detect, contest and recover from data misuse;

e) The continued risk to their PSI, and the PSI of their family members, which remains in OPM's and Treasury's possession and is subject to further unauthorized uses so long as Defendants fail to take adequate and appropriate measures to protect disclosure to DOGE-related individuals; and

f) Current and future costs in terms of time, effort, and money that will be expended to monitor, prevent, detect, contest, and repair the impact of the compromised PSI data caused by Defendants OPM and Treasury Department.

V. CLASS ALLEGATIONS

54. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and all others similarly situated. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of Rule 23.

55. The proposed class is defined as:

> **Nationwide Class:** All current, former, and prospective employees of the United States whose personal sensitive information ("PSI") was

accessed without their prior written authorization from OPM and Department of Treasury beginning in January 2025.

56. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

57. Excluded from the Class are Defendants, including Defendants' agents, officers and directors, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

58. The members of the Class are so numerous that joinder is impractical. The Class consists of thousands of members, the identity of whom is within the knowledge of and can be ascertained only by resort to OPM's records.

59. The Plaintiffs' claims are typical of the claims of the Class they seek to represent. Plaintiffs Nemeth-Greenleaf, Judkins, Michel, Nemeth, and Rifer, like all members of the class, are former, current, and prospective employees of the federal government who provided sensitive personal information to Defendants who relied to their detriment on Defendants to not provide unauthorized access to their personal information.

60. There are numerous questions of law and fact common to the Class and those common questions predominate over any questions affecting only individual Class Members.

61. Among the questions of law and fact common to the Class are:

a. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records, including unauthorized access by government and non-government employees;

b. Whether Defendants disclosed Plaintiffs' and Class Members' PSI without their prior written consent;

c. Whether Defendants' conduct was willful or with flagrant disregard for the security of Plaintiff and Class Members' PSI;

d. Whether Defendants provided unauthorized access to Plaintiffs' PSI that is stored and/or maintained through OPM and the Treasury Department;

e. Whether Defendants failed to disclose to Plaintiffs and Class Members that they provided unauthorized access to Plaintiffs' and the Class Members' PSI, including to government employees and/or non-government employees without prior written consent;

f. The proper method or methods by which to measure damages and equitable relief; and

g. Whether the Class Members are entitled to declaratory and injunctive relief.

62. Plaintiffs' claims are typical of the claims of other Class Members. Among other things, Plaintiffs and Class Members are all former, current, and prospective employees of the federal government who provided sensitive personal information to OPM and the Treasury Department as a condition of their employment, and who suffer damages as a result of Defendants providing unauthorized access to their PSI, including to non-government and unauthorized government employees without prior written approval.

63. Plaintiffs are committed to the vigorous prosecution of this action. Plaintiffs understand the nature of class action proceedings and this action specifically, and they are able and willing to fulfill the duties of class representatives. Plaintiffs have retained competent counsel experienced in the prosecution of class actions and, in particular, class actions on behalf of

government employees and regarding unauthorized access to Class Members' personal sensitive information. Accordingly, Plaintiffs are adequate representatives and will fairly and adequately protect the interests of the Class.

64. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Since the amount of each individual Class Member's claim is small relative to the complexity of the litigation, and due to the resources of Defendants, few Class Members could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the Class Members will lack a viable remedy to address Defendants' misconduct.

65. Even if Class Members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

66. Plaintiffs know of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

VI. CAUSE OF ACTION

VIOLATION OF UNITED STATES 5 U.S.C. § 552a PRIVACY ACT OF 1974 ("PRIVACY ACT") AGAINST ALL DEFENDANTS
(On Behalf of Plaintiffs and the Nationwide Class)

67. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

68. OPM and the Treasury Department are each an "agency" within the meaning of the Privacy Act.

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

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

71. OPM and the Treasury Department obtained and preserved Plaintiffs' and Class Members' PSI in a system of records during the recruiting and security check processes.

72. OPM and the Treasury Department are therefore prohibited from disclosing federal applicants' PSI under 5 U.S.C. § 552a(b) and are responsible for establishing appropriate "safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity" under 5 U.S.C. § 552a(e)(10)."

73. OPM and the Treasury Department are, and at all relevant times were required by law to comply with both FISMA and the Modernization Act. OPM and the Treasury Department are also responsible for ensuring that its cybersecurity systems comply with 5 U.S.C. § 552a and other rules and regulations governing cybersecurity practices.

74. However, through a continuous course of conduct beginning in January 2025, Defendants intentionally, willfully, and with flagrant disregard failed to administer OPM and the Treasury Department to comply with FISMA.

75. Specifically, OPM Defendants and Treasury Defendants were required—but failed—to take several steps to comply with applicable security rules and regulations including but not limited to:

a) Provide for development and maintenance of minimum controls required to protect federal information and information systems, 44 U.S.C. § 3551(3);

b) Provide a mechanism for improved oversight of federal agency information security programs, including through automated security tools to continuously diagnose and improve security, 44 U.S.C. § 3551(4);

c) Maintain "information security," defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide, in relevant part, confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, 44 U.S.C. § 3552(3)(B);

d) Ensure that all personnel are held accountable for complying with the agency-wide information security program, 44 U.S.C. § 3554(a)(7); and,

e) Ensure that all data breaches—including unauthorized disclosure or access to protected employee data, such as Plaintiffs' PSI—are reported to Congress, including information about how the breach occurred and an estimate of the number of individuals affected by the breach and assessment of risk of harm to those individuals, 44 U.S.C. § 3554(c)(1)(A)(iii).

76. Through a continuous course of conduct, the OPM Defendants and Treasury Defendants thus willfully, intentionally and with flagrant disregard refused to take steps to

implement "appropriate safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity," including by giving access to Plaintiffs' PSI data stored on OPM and Treasury Department computer systems to individuals without a lawful or legitimate need for such data, without proper security clearances to access such data, and, in some cases, without those individuals being government employees at the time of disclosure.

77. Defendants' actions resulted in (1) the disclosure of Plaintiffs and Class Members' records without prior written consent in violation of 5 U.S.C. § 552a(b) and, ultimately, (2) the "substantial harm, embarrassment, inconvenience, or unfairness" to Plaintiffs and Class Members that 5 U.S.C. § 552a(e)(10) is designed to protect against.

78. As a result of the Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the privacy act. Such damages have included or may include without limitation:

a) The loss of the opportunity to control how their PSI is used;

b) The compromise, publication, and/or theft of their PSI and the PSI of their family members;

c) Out of pocket costs associated with the prevention, detection, and recovery from identify theft and/or unauthorized use of accounts, including financial and medical accounts;

d) Lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate any consequences from the OPM and Treasury breaches, including but not limited to efforts spent researching how to prevent, detect, contest and recover from data misuse;

e) The continued risk to their PSI, and the PSI of their family members, which remains in OPM's and Treasury's possession and is subject to further unauthorized uses so long as both fail to take adequate and appropriate measures to protect disclosure to DOGE-related individuals; and

f) Current and future costs in terms of time, effort, and money that will be expended to monitor, prevent, detect, contest, and repair the impact of the compromised PSI data caused by Defendants OPM and Treasury Department.

79. Plaintiffs and Class Members are thus entitled to relief pursuant to 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class demand a jury trial on all claims so triable and judgment as follows:

1. Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' counsel to represent the Class;

2. Award Plaintiffs and Class members appropriate relief, including actual and statutory damages;

3. Award equitable, injunctive, and declaratory relief as may be appropriate;

4. Award pre-judgment interest at the maximum rate permitted by applicable law;

5. Award costs and disbursements assessed by Plaintiffs in connection with this action, including reasonable attorneys' fees pursuant to applicable law; and

6. Award such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs and all others similarly situated hereby demand trial by jury on all issues in this complaint that are so triable as a matter of right.

Dated: February 11, 2025

Respectfully submitted,

/s/ *Hassan A. Zavareei*

Hassan A. Zavareei (D.C. Bar No. 456161)
Andrea R. Gold DC (D.C. Bar No. 502607)
Gemma Seidita DC (D.C. Bar No. 1721862)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue Northwest, Suite 1010
Washington, DC 20006
(202) 919-5852
hzavareei@tzlegal.com
agold@tzlegal.com
gseidita@tzlegal.com

Cort T. Carlson (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
(510) 254-6808
ccarlson@tzlegal.com

Gregory McGillivary (D.C. Bar No. 411029)
Sara L. Faulman (D.C. Bar No. 496679)
John W. Stewart (D.C. Bar No. 1028836)
Sarah M. Block (D.C. Bar No. 1026577)
McGILLIVARY STEELE ELKIN LLP
1101 Vermont Ave. NW
Suite 1000
Washington, DC 20005
(202) 833-8855
gkm@mselaborlaw.com
slf@mselaborlaw.com
jws@mselaborlaw.com
smb@mselaborlaw.com

Attorneys for Plaintiffs and the Proposed Class