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,

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

Defendants.

Case No. 1:25-cv-00407 (CRC)

FIRST AMENDED CLASS ACTION COMPLAINT

FIRST AMENDED 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") and Defendant United States Department of the Treasury ("Treasury Department") (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 "PSI")—contained in Defendants' records to non-governmental employee and private citizen Elon Musk, as well as

[1] Pursuant to Local Civil Rule 5.1(c)(1), a notice containing the required information for each Plaintiff was filed under seal at Docket Entry ("Dkt.") 6.

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

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.

5. Indeed, Defendants' actions—which are ongoing—have already compromised Plaintiffs' and Class Members' PSI. For example, Plaintiff Rifer has been notified that his personal email address has been disclosed on the dark web, along with a strong possibility that the linked

password and other personal information might be compromised as well. The email address found on the dark web has been on file with USAID and has been regularly used by the Government to communicate with Plaintiff Rifer, particularly in recent months. Likewise, Plaintiff Nemeth-Greenleaf received notification that her email address, which is on file with the Department of the Navy, has also been disclosed on the dark web. Defendants' unwillingness to acknowledge, let alone correct, their misconduct only compounds the harms they have caused Plaintiffs and Class Members.

II. JURISDICTION AND VENUE

6. 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).

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

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

9. 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.

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 Treasury Department 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.

14. 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 services from Aura Identity Protection.

15. 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 Defendants' breaches of his PSI from media reports. In response, Plaintiff Judkins purchased credit and identity theft protection services from Aura Identity Protection.

16. 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.

17. Plaintiff Donna Nemeth is a resident of the State of Colorado. She was employed at all times material with the United States Department of Agriculture, Forest Service, at the Rocky Mountain Regional Office, where she worked 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 services from Aura Identity Protection.

18. 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 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

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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 was originally 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. At the time Defendants illegally disclosed Plaintiffs' and Class Members' PSI to DOGE agents, DOGE did not maintain any public security policies, Defendants did not provide security training to DOGE agents before disclosing Plaintiffs' and the Class Members' PSI, and Defendants did not vet or otherwise investigate whether it was lawful for them to access Plaintiffs' and Class Members' PSI entrusted to them.

28. In late January, 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.

29. Days after being sworn in as Secretary of the Treasury, Scott 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. 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.

30. 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 of Musk's 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] Mr. Elez later sent an unencrypted spreadsheet with personal information to individuals outside of the Treasury Department.[4]

31. 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 Musk is the Chief Executive Officer. Although Defendant Scales neither had the requisite

[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), perma.cc/F7BF-DZVX.

[4] Wes Davis, THE VERGE, "A DOGE staffer broke treasury policy by emailing unencrypted personal data" (Mar. 15, 2025), perma.cc/M6AA-3BMU.

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.

32. Defendants then improperly granted other DOGE-affiliated individuals, including Musk, full access to OPM's data and the 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. These improperly accessed systems included at least the following: Enterprise Human Resources Integration; Electronic Official Personnel Folder; USAJOBS; USA Staffing; USA Performance; and Health Insurance (which houses information about the Federal Employee Health Benefits (FEHB) program and the Postal Service Health Benefit (PHSB) program.[5]

33. 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 Musk nor these individuals have proper security clearance to access these data or systems.

34. 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

[5] Caleb Acarma and Judd Legum, MUSK WATCH, "Musk associates given unfettered access to private data of government employees" (Feb. 3, 2025), perma.cc/EGH2-HWHE.

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.[6] In addition, as recently as 2023, Mr. Coristine ran a company that provided support to a cybercrime gang that has bragged about trafficking in stolen data.[7]

35. These actions represent "a dramatic shift in the way the government's business has traditionally been conducted."[8] Normally, access to government databases is highly restricted, with strict, differential controls on what a government employee, contractors, and civil-service 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*.[9]

36. 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."[10] From a security perspective, that Defendants have allowed these individuals access likely without proper security clearances is "madness."[11]

37. 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

---

[6] Jason Leopold *et al.*, BLOOMBERG, "Musk's DOGE teen was fired by cybersecurity firm for leaking company secrets," (Feb. 7, 2025), perma.cc/7N54-FA5F.
[7] Reuters, THE GUARDIAN, "Teen member of Musk's Doge staff provided tech support to cybercrime ring, records show" (Mar. 26, 2025), perma.cc/HNY4-NV7C.
[8] Charlie Warzel and Ian Bogost, THE ATLANTIC, "The Government's Computing Experts Say They Are Terrified," (Feb. 7, 2025), perma.cc/6XFF-75N6.
[9] *See id*.
[10] *Id*.
[11] *Id*.

users, as reports indicate that certain individuals, including Elez, were also provided with "write" access[12]—"Musk's people could easily find individuals in databases or clone entire servers and transfer that secure information somewhere else."[13] And whatever data is siphoned now, including Plaintiffs' PSI, "could be [Musk's] forever."[14]

38. Such access and disclosure to persons without proper vetting or training makes Plaintiffs' and Class Members' PSI more vulnerable to hacking, identify theft, and other malicious activity by foreign adversaries or other malignant actors.

39. This access is also plainly unlawful.

40. 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.

41. 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.

42. For example, representatives from U.S. DOGE Service have fed sensitive data from across the U.S. Department of Education into artificial intelligence software to probe the agency's programs and spending.[15] 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

[12] Victoria Elliott, Leah Feiger, and Tim Marchman, WIRED, "The US Treasury Claimed DOGE Technologist Didn't Have 'Write Access' When He Actually Did" (Feb. 6, 2025), perma.cc/A8T4-E9Q6.
[13] Charlie Warzel and Ian Bogost, THE ATLANTIC, "The Government's Computing Experts Say They Are Terrified," (Feb. 7, 2025), perma.cc/6XFF-75N6.
[14] *Id*.
[15] Hannah Natanson *et al.*, THE WASHINGTON POST, "Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts," (Feb. 6, 2025), perma.cc/3JGS-FUHR.

grants, as well as sensitive internal financial data[.]"[16] 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.[17]

43. In fact, following a lawsuit from 19 state attorneys general against President Donald Trump, and Defendant Treasury Department, 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.[18]

44. One June 9, 2025, in a lawsuit against OPM, another federal district court judge granted a preliminary injunction, finding the plaintiffs "have shown irreparable harm due to both

---

[16] *Id*.
[17] *Id*.
[18] *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.). While the court found that the states themselves were not within the zone of interest as individuals whom the Privacy Act was intended to protect, the court granted a preliminary injunction after evaluating the states' claim under the Administrative Procedure Act. *Id.* at Dkt. 76. The Court held that the states were more likely than not to succeed on their claims and demonstrated a "substantial risk of future harm where the data access protocols in place do not satisfactorily vet the employees with access and rigorously train them in data security measures." Dkt. 76 at 50, 51. The court further concluded that the plaintiffs, more likely than not, would show "the agency's processes for permitting the Treasury DOGE Team access to critical BFS payment systems, with full knowledge of the serious risks that access entailed, was arbitrary and capricious." Dkt. 76 at 50. Finally, the court noted that failing to correct the significant security concerns could result in a "catastrophic" cybersecurity breach. Dkt. 76 at 61.

the unlawful disclosure of OPM records to employees working on the DOGE agenda and the increased risk to cybersecurity because of their unlawful disclosure . . . The defendants have not identified any credible need that the DOGE agents had for the access to OPM systems that they were given and the plaintiffs have shown that it is exceedingly unlikely that there was any such need."[19]

45. Just as these courts have recently recognized, the threat of further disclosure and use of sensitive employee data, including that of the Plaintiffs and Class Members, is real.

46. OPM's data has been and continues to be a target of foreign adversary actors to the detriment of those whose data is compromised.

47. For example, in 2015, foreign adversary hackers allegedly working on behalf of the Chinese government carried out a large attack on OPM, exfiltrating information belonging to approximately 4.2 million federal workers and an additional 21.5 million people who had undergone background checks and security clearances. The attack was considered to be "one of the most damaging on record because of its scale and, more importantly, the sensitivity of the material taken."[20]

48. Shortly after OPM's unlawful disclosure of Plaintiffs' and Class Members' PSI, the Washington Post reported that the access raised an expert's concern "that Russia, China, Iran, and other adversaries could seek to exploit the chaos by launching new cyber intrusions or targeting the devices and communications of Musk's [DOGE] team."[21] Another expert commented: "If I

---

[19] *Am. Fed'n of Gov't Emps., AFL-CIO et al. v. U.S. Off. of Pers. Mgmt. et al.*, 1:25-cv-01237-DLC, ECF No. 121 at 94-95 (S.D.N.Y.)

[20] Patricia Zengerle, Megan Cassella, REUTERS, "Millions more Americans hit by government personnel data hack" (July 9, 2015), https://archive.is/22VG6.

[21] Isaac Stanley-Becker, Greg Miller, Hannah Natanson, and Joseph Menn, WASHINGTON POST "Musk's DOGE agents access sensitive personnel data, alarming security officials" (Feb. 6, 2025), perma.cc/EGH2-HWHE.

were a nation like China, Russia, or Iran, I'd be having a field day with a bunch of college kids running around with sensitive federal government data on unencrypted hard drives."[22]

49. In May 2025, National Labor Relations Board (NLRB) Information Technology staffer Daniel Berulis revealed through a whistleblower disclosure made to Congress and the U.S. Office of Special Counsel, eventually shared with NPR, that following DOGE's access to NLRB internal systems, suspicious log-in attempts to the NRLB's secure systems were made by an IP address in Russia and there was a spike in data leaving the agency.[23] Mr. Berulis, who is described as a "DevSecOps Architect" with "almost two decades of experience" described how DOGE's activity "resulted in a significant cybersecurity breach that likely has and continues to expose our government to foreign intelligence and our nation's adversaries."[24]

50. Specifically, as supported by his sworn declaration, Mr. Berulis details his concern that "within minutes of DOGE personnel creating user accounts in NLRB systems, on multiple occasions someone or something within Russia attempted to login using all of the valid credentials (eg. Usernames/Passwords)[,]" combined with "verifiable data being systematically exfiltrated to unknown servers within the continental United States – and perhaps abroad[.]" *Id*. at 2.

51. The Berulis Disclosure further demonstrates that Defendants' conduct violated and continues to violate the Federal Information Security Modernization Act ("FISMA") and guidelines set forth by the Cybersecurity and Infrastructure Security Agency ("CISA") and

---

[22] *Id.*

[23] Jenna McLaughlin, NPR, "A whistleblower's disclosure details how DOGE may have taken sensitive labor data" (Apr. 15, 2025), perma.cc/ZDT8-FW5T.

[24] Daniel Berulis, Whistleblower Aid Protected Whistleblower Disclosure, "Dan Berulis Disclosure: Cyber Security Brach and Data Exfiltration through DOGE Systems and Whistleblower/Witness Intimidation," (hereinafter "Berulis Disclosure") (last accessed June 27, 2025), perma.cc/8EC9-8BMU.

National Institute of Standards and Technology ("NIST"), thereby exposing Privacy Act-protected information in violation of the Act.

52. Mr. Berulis describes how beginning in March 2025, DOGE staffers arrived at NLRB offices but "interacted with only a small group of NLRB staff, never introducing themselves to those of us in Information Technology," *Id*. at Exhibit A, Berulis Decl. ¶ 6, proof that DOGE did not comply with cybersecurity mandates, including by not coordinting with cybersecurity subject area expertise at NLRB, including Mr. Berulis. Indeed, Mr. Berulis—who had oversight over day-to-day cybersecurity operations at NLRB—was instructed "*not* to adhere to SOP [standard operating procedure] with the doge [*sic*] account creation in regards to creating records[,]" including that "there were to be no logs or records made of the accounts created for DOGE employees," despite that "DOGE officials required the highest level of access and unrestricted access to internal systems." *Id*. ¶ 7 (emphasis added). In Mr. Berulis's words, "we were to hand over any requested accounts [to DOGE staffers], stay out of DOGE's way entirely, and assist them when they asked. We were further directed not to resist them in any way or deny them any access." *Id*.

53. Without standard cybersecurity protections and departing from agency standard operating procedures, DOGE staffers obtained "tenant owner" level accounts "with essentially unrestricted permission to read, copy, and alter data." *Id*. DOGE staffers obtained this unfettered, unmonitored access despite that other, safer, alternatives were available. Indeed, Mr. Berulis explained that DOGE staffers could have used "roles that auditors can use and have used extensively in the past but would not give the ability to make changes or access subsystems without approval." *Id*. Instead, the suggestion that DOGE staffers use such auditor accounts "was not open to discussion." *Id*.

54. DOGE's unfettered access using largely unmonitored "tenant admin accounts" exposed sensitive, personally identifiable information to inordinate risk of compromise. For example, Mr. Berulis described how "tenant admin accounts that are compromised typically are leveraged by attackers to perform various actions and *hide* them from defenders…" *Id*. (emphasis added). "According to Microsoft documented best practices tenant admin permissions should never be assigned to auditors because it can mask actions like creating or deleting accounts, changing role assignments, or altering policies and far exceeds any legitimate job need." *Id*.

55. After DOGE obtained such access, on March 4, 2025, Mr. Berulis began to see signs of nefarious activity in NLRB's systems. These signs included *inter alia* "discovery of an anomalous 'container' record and unexpectedly expired storage tokens," which could aid an attacker "to work invisibly, leaving little to no obvious trace of their activities once removed," as well as the fact that "unknown (or deleted) accounts created access keys for resources in the subscriptions under the tenant." *Id*. ¶ 8.

56. The next day, Mr. Berulis noticed another "anomaly"—"there was a large section of missing records in relation to recently created network resources and a network watcher in Azure [a system software program] was in the 'off' state, meaning it wasn't collecting or recording data like it should have." *Id*. at ¶ 9. Around the same time, Mr. Berulis noticed data had been transferred out of the NLRB network which was "odd" because there was no corresponding inbound data spike, which would be expected if the data transfer were authorized as in patching or other normal conditions. *Id*. at ¶ 10.

57. Below is an image of the large data export that Mr. Berulis noticed on March 5, 2025, suggesting nefarious activity:

Id.

58. Mr. Berulis described further unusual activity on or about March 6, 2025, namely that "at least one account's naming structure suggested that it might have been created and later deleted for DOGE to use in the NLRB's cloud systems, hosted by Microsoft: 'DogeSA_2d5c3e0446f9@nlrb.microsoft.com.'" *Id*. at ¶ 12.

59. Critically, Mr. Berulis expressed concern that DOGE's actions in this respect is and was not "audited" and departed from "mandate[d]" standard operating procedure, including that multi-factor authentication requirements were simultaneously disabled for certain mobile devices, which he found "odd because we have a mandate that it be on, and that is the first time I have ever seen it in an off state." *Id*.

60. These and other odd occurrences culminated in Mr. Berulis "tracking what appeared to be sensitive data leaving the secured location it is meant to be stored." *Id*. ¶ 18.

Specifically, "he initially saw gigabytes exiting the NxGen case management system 'nucleus,' within the NLRB system, and [ ] later witnessed a similar large spike in outbound traffic leaving the network itself." *Id*. The data exfiltrated without explanation and in a suspicious manner amounted to around 10 gigabytes, or the "equivalent of a full stack of encyclopedias" if the data was printed as text. *Id*. This was "extremely unusual because data almost never directly leaves NLRB's databases." *Id*.

61. Mr. Berulis was especially alarmed by this exfiltration of sensitive data because it followed DOGE's unprecedented access to NLRB's systems and because in the days after DOGE accessed NLRB's systems a user with an IP address in Russia attempted to log in to NLRB's systems, meaning that the systems were at heightened risk of attack. *Id*. at ¶ 21.

62. "Whoever was attempting to log in was using one of the newly created accounts that were used in the other DOGE related activities and it appeared they had the correct username and password…" *Id*. "There were more than 20 such attempts, and what is particularly concerning is that many of these login attempts occurred within 15 minutes of the accounts being created by DOGE engineers." *Id*.

63. Following the initial exfiltration of data, on or about March 13, 2025, Mr. Berulis discovered a connection record in a network watcher showing that data had been transferred to an unknown external endpoint. *Id*. at ¶ 22. The database affected by suspicious activity "contains not only PII of claimants and respondents with pending matters before the agency, but also many other businesses confidential internal processes and information gathered or provided during investigations and litigation that were not intended for public release." *Id*. at ¶ 27.

64. Mr. Berulis and ACIO of Security, Chris L., concluded that the foregoing should be reported to CISA "Us-Cert", U.S. Computer Emergency Readiness Team, to conduct an

interagency forensic investigation, such as was conducted in connection with the 2015-2016 OPM data breach. This course of action was taken because the foregoing "met the criteria to trigger our standard operating procedure regarding *theft* of data." *Id*. at ¶ 25 (emphasis added).

65. However, on or around April 3 or 4, 2025, Mr. Berulis and ACIO of Security Chris L. "were informed that instructions had come down to drop the US-Cert reporting and investigation and we were directed not to move forward or create an official report." *Id*. at ¶ 26.

66. This was counter to the findings of Mr. Berulis, who, based on his training and experience, concluded that a data breach was facilitated by an internal actor. *Id*. ¶ 27. The activity Mr. Berulis observed, in his professional opinion, "aligns directly with behavior of attackers according to the MITRE ATT&CK Framework and are the exact behaviors (Indicators of Compromise) of one who was trying to erase records of activities, retard detection, and covertly hide what data was being extracted after the fact." *Id*.

67. The foregoing motivated Mr. Berulis to disclose this information to the U.S. Senate Select Committee on Intelligence on April 14, 2025. Concerningly, while preparing the Berulis Disclosure, "someone physically taped a threatening note to Mr. Berulis' home door with photographs – taken via a drone – of him walking in his neighborhood." *Id*. The threatening note made clear reference to the disclosure he was preparing. *Id*. The Berulis Disclosure believes the threat "involved someone with the ability to access NLRB systems." *Id*.

68. The Berulis Disclosure is proof of the ongoing harms and risks of harm that DOGE's unprecedented misconduct—as permitted by federal agencies, including Defendants—causes to government data systems that have been accessed without authorization.

69. Indeed, the Berulis Disclosure supports that it is federal agencies' new policy and practice to order that DOGE be provided with unfettered, unmonitored, and fundamentally

insecure access to agency data systems containing sensitive information including PSI without prior or lawful authorization from those affected, and to allow DOGE-affiliated individuals—and potentially bad actors—to exfiltrate large amounts sensitive information in a manner that is neither authorized by law nor in line with cybersecurity best practices.

70. Further, the Berulis Disclosure reveals that without a whistleblower disclosure, the public likely would not have learned of federal agencies' granting DOGE unprecedented and reckless access to sensitive government data systems and misconduct regarding same.

71. As such, it is reasonable to conclude that other agencies, including Defendants OPM and the Treasury Department, have instituted this policy and practice of ordering that DOGE-affiliated individuals be provided unmonitored, unfettered access to government data systems, including the power to access, obtain, edit, and exfiltrate large amounts of sensitive government data, including Plaintiffs' and Class Members' PSI, without lawful authorization and at extreme risk that such data would fall and has fallen into the hands of third party bad actors, including foreign adversaries.

72. Further, on April 8, 2025, the Office of the Comptroller of the Currency ("OCC"), an independent bureau of Defendant Department of Treasury, formally notified Congress that it had identified a February 2025 breach of the OCC's email system, when an unauthorized user accessed OCC user accounts, including emails and attachments, via a service account with administrative level privileges.[25] A follow-up letter from the OCC dated April 14, 2025, provided further detail about the "major incident resulting from a breach of the OCC's email system" and that the "unauthorized access involved sensitive information."[26] Journalists have reported that in

[25] Office of the Comptroller of the Currency, Letter re: OCC Information Security Incident (April 14, 2025), perma.cc/8ZXJ-6WS6.
[26] *Id.*

February 2024, the attackers accessed around 150,000 emails including those from approximately 100 bank regulators.[27]

73. In mid-April 2025, an employee at the General Services Administration discovered that transceivers made and operated by Starlink—a company owned by SpaceX, which Musk founded—had been installed on the Agency's rooftop with wires snaking into the administrator's office window, likely for the purpose of siphoning off agency data.[28]

74. Reports reveal that DOGE intends to unify all federal employee data, including PSI, into a central hub and has removed protections around sensitive information, for example on Social Security numbers, birth dates, employment history, and disability and medical records. According to cybersecurity experts interviewed by The Washington Post, such a consolidation of data greatly increases the risk of exposing data to hackers. Jake Williams, a former National Security Agency hacker who is the vice president of Hunter Strategy, stated that combining a tempting target with security shortcuts like those implemented by DOGE compounds the risk that China—the mastermind of the previous data breach at OPM—will attempt another cyberattack.[29]

75. On May 8, 2025, Ars Technica reported that login credentials belonging to a DOGE employee who also worked at the Cybersecurity and Infrastructure Security Agency (CISA) have appeared in public leaks from info-stealer malware, "a strong indication" that his devices have been recently hacked. This indicates that if the employee used the same or similar credentials to

[27] Lauren Yocono, CIMCOR, "OCC Cyber Breach: Undetected for 8 Months, Exposing Sensitive Data" (May 6, 2025), perma.cc/K6KG-WK87.
[28] Byron Tau et al., THE ASSOCIATED PRESS, "Elon Musk installed his top lieutenants at a federal agency you probably haven't heard of" (Apr. 17, 2025), https://archive.ph/UFR8s; Office of Senator Elizabeth Warren, "Special Interests Over the Public Interest: Elon Musk's 130 Days in the Trump Administration" (June 2025), at 8, perma.cc/PAH6-EVAC.
[29] Hannah Natanson, *et al.*, THE WASHINGTON POST, "DOGE aims to pool federal data, putting personal information at risk (May 7, 2025), https://archive.is/j8Xg5.

access government systems through his work with DOGE, cyber attackers could have already accessed any sensitive or personal information to which the employee had access.[30]

76. This unlawful and flagrant intrusion into federal employees' privacy is unprecedented.

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

77. 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.

78. 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.

79. 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.

80. 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."

[30] Dan Goodin, ARS TECHNICA, "DOGE software engineer's computer infected by info-stealing malware" (May 8, 2025), https://archive.is/sjZ5U.

81. Plaintiffs reasonably fear harmful consequences of the disclosure and use of their PSI. Notably, President Trump, former DOGE director Musk, and others have threatened to fire government employees viewed as disloyal. Defendants' disclosure of Plaintiffs' PSI puts Plaintiffs' job security at risk. Moreover, employees of certain federal agencies, such as USAID, have had their personal safety placed at risk because they work or have worked in fields where public disclosure of their PSI could lead to retaliation from those who oppose their agency's work or because they work in countries where knowledge of their PSI could be used to harm, threaten, or extort them.

82. Plaintiffs have, and will continue to, experience harmful exposure of their personal data as a result of Defendants' actions.

83. For example, on May 27, 2025, McAfee—which performs periodic scans of the dark web as a part of its computer virus protection and digital security plans—notified Plaintiff Rifer that his personal email address has been disclosed on the dark web, along with a "strong possibility" that the linked password and other personal information might be compromised as well. The email address found on the dark web has been on file with USAID and has been regularly used by the Government to communicate with Plaintiff Rifer, particularly in recent months. It is therefore reasonable to conclude that Defendants' misconduct caused Plaintiff Rifer's PSI to be exposed to the dark web.

84. Additionally, Plaintiff Nemeth learned on April 20, 2025, that an apparent identity thief had made two fraudulent purchases, one on April 2, 2025, and another on April 16, 2025, using a Citi Visa credit card in Plaintiff Nemeth's name.

85. Another plaintiff, Plaintiff Nemeth-Greenleaf, recently learned that an apparent identity thief had made a fraudulent purchase using a Lighthouse Credit Union debit card in her

name between approximately April 4 and April 15, 2025. This Credit Union account information was on file with the Defendants at the time of the improper disclosures, as it is the account into which Plaintiff Nemeth-Greenleaf's paycheck is deposited by direct deposit each pay period. Plaintiff Nemeth-Greenleaf has also received notification from Aura that her personal email address, which is on file with the Department of the Navy and regularly used to communicate with Plaintiff Nemeth-Greenleaf, had been disclosed on the dark web. But for Defendants' unlawful conduct, Plaintiff Nemeth-Greenleaf's PSI would not have been compromised and used to effectuate fraudulent, harmful injury-causing transactions, as occurred.

86. Further, Defendants have refused to acknowledge or remedy the unauthorized access alleged herein, providing no assurance that going forward access will only be given to OPM and Treasury Department systems containing PSI to those who are authorized to have access under the Privacy Act. As such, Defendants' misconduct—which is ongoing—only magnifies the cybersecurity harms to Plaintiffs, and the risk of same.

87. 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

88. 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.

89. 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.

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

91. 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.

92. 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 Defendants' records.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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)

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

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

103. 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."

104. 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."

105. 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.

106. 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)."

107. 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.

108. 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.

109. 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).

110. 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.

111. Such disclosure of Plaintiffs' and Class Members' PSI was not necessary for the performance of any lawful duty by Defendants.

112. Upon information and belief, when Defendants disclosed Plaintiffs' and Class Members' PSI to Defendants, they were fully aware that DOGE did not have a lawful basis to access that information.

113. 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.

114. 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) Intrusion upon their otherwise private affairs and concerns;

d) 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;

e) 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;

f) 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

g) 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.

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

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

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

Dated: June 30, 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