UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ANDREA GRIBBON,

CHERICE PRATER,

HELGA HERTLEIN,

DONALD CUSTER,

LYNN BOISROND,

and

DENNIS TITKO,

on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

ELON MUSK,

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

THE DEPARTMENT OF THE TREASURY
1500 Pennsylvania Ave NW
Washington, DC 20220

and

SCOTT BESSENT,
in his official capacity as Secretary of the Treasury,

Defendants.

Case No. 1:25-cv-00422

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

1. Plaintiffs ANDREA GRIBBON, CHERICE PRATER, HELGA HERTLEIN, DONALD CUSTER, LYNN BOISROND, and DENNIS TITKO file this action against ELON MUSK, THE UNITED STATES OFFICE OF PERSONNEL MANAGEMENT ("OPM"), the DEPARTMENT OF THE TREASURY (the "Treasury") and SCOTT BESSENT, in his official capacity as Secretary of the Treasury, for damages resulting from Defendants' unlawful ongoing, systematic, and continuous disclosure of personal and financial information contained in Defendants' records to Elon Musk and other members of the so-called "Department of Government Efficiency" ("DOGE").

2. Millions of individuals engage in financial transactions with the federal government. The government collects trillions of dollars from individuals who pay their income taxes, obtain government services, and pay back loans and other debts that they owe. People also receive money from the federal government. Social Security retirement and disability payments, federal tax refunds, veterans' benefits, and salaries and wages for federal workers are some examples of payment transactions that occur between ordinary individuals and federal agencies.

3. The job of effectuating these financial transactions for the federal government belongs to the Treasury (operating through the Bureau of the Fiscal Service (the "Bureau"). To carry out its duties, the Treasury collects and maintains sensitive personal and financial information about the individuals who are the counterparties to the transaction. Names, Social Security numbers, birth dates, birth

places, home addresses and telephone numbers, email addresses, and bank account information about millions of individuals are maintained within the Treasury's records to enable the secure and timely transfer of funds between federal agencies and members of the public.

4. Federal laws protect sensitive personal and financial information from improper disclosure and misuse, including by barring disclosure to individuals who lack a lawful and legitimate need for it.

5. In his first week as Treasury Secretary, Defendant Bessent violated these restrictions. Elon Musk and/or other DOGE members had sought access to the Bureau's records for some time, only to be rebuffed by the employee then in charge of the Bureau. Within a week of being sworn in as Treasury Secretary, Mr. Bessent placed that civil servant on leave and granted DOGE-affiliated individuals full access to the Bureau's data and the computer systems that house them. He did so without making any public announcement, providing any legal justification or explanation for his decision, or undertaking the process required by law for altering the agency's disclosure policies.

6. The scale of the intrusion into individuals' privacy is massive and unprecedented. Millions of people cannot avoid engaging in financial transactions with the federal government and, therefore, cannot avoid having their sensitive personal and financial information maintained in government records. Secretary Bessent's action granting DOGE-affiliated individuals full, continuous, and ongoing access to that information for an unspecified period of time means that retirees,

taxpayers, federal employees, companies, and other individuals from all walks of life have no assurance that their information will receive the protection that federal law affords. And because Defendants' actions and decisions are shrouded in secrecy, individuals will not have even basic information about what personal or financial information that Defendants are sharing with outside parties or how their information is being used.

7. People who must share information with the federal government should not be forced to share information with Elon Musk or his "DOGE." And federal law says they do not have to. The Privacy Act of 1974 generally, and the Internal Revenue Code with respect to taxpayer information, make it unlawful for Secretary Bessent to hand over access to the Bureau's records on individuals to Elon Musk or other members of DOGE. Plaintiffs file this action to recover damages resulting from Defendant's systematic, continuous, and ongoing violation of federal laws that protect the privacy of personal information contained in federal records, including but not limited to reimbursement of the cost of credit monitoring and identity protection services.

JURISDICTION AND VENUE

8. This Court has statutory jurisdiction over this action pursuant to 28 U.S.C. § 1331, because this action arises under the laws of the United States.

9. Venue is proper in this judicial district under 28 U.S.C. § 1391(e)(1)(A) because Defendants are officers and agencies of the United States and because at least one defendant resides in Washington, D.C.

PARTIES

10. Plaintiff Andrea Gribbon is a resident of the state of Washington. She is currently on federal disability and receives regular payments from the United States. In order to receive disability, Gribbon had to provide the United States with her Personal Sensitive Information ("PSI"), including her name, address, birth date and Social Security number. Plaintiff Gribbon learned about Defendants' breaches of her PSI from media reports. In response, Plaintiff Gribbon purchased credit and identity theft monitoring through Experian.

11. Plaintiff Cherice Prater is a resident of Florida. She is unemployed. Plaintiff Prater receives retirement benefits from OPM due to her deceased husband's 11.5 years of military service and 20 years with the U.S. Postal Service. She also receives disability through the Treasury. In order to receive these payments, Prater had to provide the United States with her Personal Sensitive Information ("PSI"), including her name, address, birth date and Social Security number. Prater learned about Defendants' breaches of her PSI from media reports. In response, Plaintiff Prater purchased credit and identity theft monitoring through LifeLock.

12. Plaintiff Helga C. Hertlein is a resident of Indiana. Plaintiff Hertlein is a United States taxpayer who, in the regular course of filing her tax returns, provided the Treasury with her Personal Sensitive Information ("PSI"), including her name, address, birth date and Social Security number. Plaintiff Hertlein learned about Defendants' breaches of her PSI from media reports. In response, Plaintiff Hertlein purchased credit and identity theft monitoring through LifeLock.

13. Plaintiff Donald Robert Custer, III, is a resident of Colorado. Plaintiff Custer is a United States taxpayer who, in the regular course of filing his tax returns, provided the Treasury with his Personal Sensitive Information ("PSI"), including his name, address, birth date and Social Security number. Plaintiff Custer learned about Defendants' breaches of his PSI from media reports. In response, Plaintiff Custer purchased credit and identity theft monitoring through Experian.

14. Plaintiff Lynn Boisrond is a resident of New York. Plaintiff Boisrond at all times relevant to this complaint currently or formerly has received student loans through the government. In the regular course of applying for government financial aid Plaintiff Boisrond provided her Personal Sensitive Information ("PSI") including her name, address, date of birth, driver's license number, and Social Security number. to the Department of Education. Boisrond learned about Defendants' breaches of her PSI from media reports. On February 1, 2025, Boisrond received an alert of an unauthorized attempted charge to her Capital One account in the amount of $35.00. Additionally, Plaintiff Boisrond was notified that her email, date of birth, and address was found on the dark web. In response, Plaintiff Boisrond purchased credit monitoring through LifeLock.

15. Plaintiff Dennis Titko is a resident of Oregon. Plaintiff Titko is a United States taxpayer who, in the regular course of filing his tax returns, provided the Treasury with his Personal Sensitive Information ("PSI"), including his name, address, birth date and Social Security number. Titko learned about Defendants' breaches of his PSI from media reports. On February 11, 2025, Titko was notified by

Wells Fargo that an account had been opened in his name. Titko did not open an account with Wells Fargo. Titko spent time communicating with Wells Fargo to alert them to this fraud attempt and close the fraudulent account. Plaintiff Titko upgraded his credit and identity theft monitoring service with LifeLock.

16. Defendant Elon Musk resides in Austin, Texas and is a businessman and executive at various companies, including Tesla, Inc. ("Tesla"), where Musk serves as CEO. On or about November 13, 2024, Musk was named by then President-elect Donald Trump to co-lead the Department of Governmental Efficiency or "DOGE". This new role is not an official government position. At all times relevant to this complaint Musk has acted as a private citizen.

17. Defendant United States Department of Personnel Management is an agency of the United States, headquartered in Washington, D.C.

18. Defendant Department of the Treasury is an agency of the United States, headquartered in Washington, D.C.

19. Defendant Scott Bessent is the Secretary of the Treasury.

FACTS

Defendants' Collection and Maintenance of Information on Individuals

20. Defendants are responsible for managing the finances of the United States Government. Their responsibilities include collecting receipts owed to the government and making payments to recipients of public funds. 31 U.S.C. §§ 3301, 3321. In fiscal year 2024, the Treasury processed nearly $5 trillion in receipts, including $2.4 trillion from individual income taxes, $1.7 trillion from Social Security

taxes, and $530 billion from corporate income taxes. In that fiscal year, the Treasury handled $6.752 trillion in outlays, including $1.46 trillion for Social Security payments and $874 billion in defense spending.[1] The U.S. Treasury is the largest collections, payments, cash management, and financial operation in the world.

21. To engage in financial transactions with individuals, Defendants must collect and maintain personal and financial information about those individuals. As federal agencies, the Treasury and the Bureau are subject to the requirements of the Privacy Act, 5 U.S.C. § 552a, with respect to records that it maintains on individuals.

22. 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.

23. 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,

[1] U.S. DEP'T OF TREAS., BUR. OF FISCAL SERV., *Final Monthly Treasury Statement, Receipts and Outlays of the United States Government For Fiscal Year 2024 Through September 30, 2024, and Other Periods* 4.

and more.

24. 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.

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. The Privacy Act prohibits the disclosure of a record about an individual to any person or another agency unless "the individual to whom the record pertains" consents or a statutory exception applies. 5 U.S.C. § 552a(b).

27. Because Defendants process tax-related transactions, they are also subject to the confidentiality requirements of the Internal Revenue Code, 26 U.S.C. § 6103. Section 6103 provides that "[r]eturns and return information shall be confidential," and cannot be disclosed by a federal officer and employee unless authorized by statute. Return and return information includes the taxpayer's identity, mailing address, taxpayer identification number, claims for refund, and other

information on tax returns. *Id.* § 6103(b)(1), (2), (6). The officers and employees of the Treasury may access return and return information if their "official duties require such inspection or disclosure for tax administration purposes." *Id.* § 6103(h)(1).

Defendants' Disclosure of Bureau Records on Individuals to DOGE

28. Beginning shortly after the inauguration of President Donald Trump on January 20, 2025, Defendants OPM and Treasury 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.

29. President Trump was inaugurated as President on January 20, 2025. The same day, he issued an executive order establishing a so-called "Department of Government Efficiency." Under the executive order, the United States Digital Service was renamed the United States DOGE Service (USDS), and a "temporary organization" was established under 5 U.S.C. § 3161 entitled "the U.S. DOGE Service Temporary Organization."

30. The executive order directs the USDS Administrator to "work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." It also directs agency heads to "take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems." The executive order "displaces all prior executive orders and

regulations, insofar as they are subject to direct presidential amendment, that might serve as a barrier to providing USDS access to agency records and systems as described above."

31. Since his inauguration, President Trump has not formally identified the individual who would serve as USDS Administrator or the full list of individuals that are part of the U.S. DOGE Service Temporary Organization.

32. During the presidential campaign, President Trump announced that billionaire entrepreneur Elon Musk would have a leadership role in DOGE. It is widely reported that, since the inauguration, Mr. Musk has played a leadership role in DOGE activities across the federal government.

33. The Trump administration has not publicly revealed whether Mr. Musk has been made an officer or employee of the U.S. government or remains a private citizen. The Trump administration also has not publicly revealed the employment status of other individuals who are part of DOGE.

34. Sometime after November 5, 2024, DOGE representatives reportedly approached officials in the Treasury seeking access to the agency's payment systems. DOGE's efforts to obtain access continued after President Trump's inauguration.

35. Initially, DOGE's requests for access to the Treasury's payment systems were reportedly rebuffed by David A. Lebryk, the highest-ranking career official at the agency and the individual who had been in charge of the Bureau. According to press reports, Mr. Lebryk advised DOGE representatives during the transition period that the information contained in the payment systems was proprietary and should

not be shared outside of the government.

36. On January 27, 2025, the Senate confirmed Mr. Bessent as President Trump's Treasury Secretary, and he was sworn in the following day. On information and belief, Secretary Bessent and his chief of staff Dan Katz had a meeting with Mr. Lebryk later that week, after which Mr. Lebryk was placed on administrative leave. On Friday, January 31, Mr. Lebryk announced that he was retiring from the Treasury after 35 years in federal service.

37. On information and belief, on Friday evening, January 31, Defendant Bessent gave representatives of DOGE full access to the federal payment system.[2] Senator Ron Wyden, Ranking Member of the Senate Committee on Finance, has reported that DOGE's access to Treasury's payment system is complete. He has stated that DOGE has "*full* access to this system. Social Security and Medicare benefits, grants, payments to government contractors…. All of it."[3]

38. Defendants have not released the full list of DOGE-affiliated individuals who have been provided access to the Treasury's payment systems, or whether those individuals are employees of the Bureau, the Treasury, another agency, or a private enterprise. Tom Krause, the Chief Executive Officer of Cloud Software Group (according to that company's website, *see* https://www.cloud.com/leadership (Feb. 3,

[2] Andrew Duehren et al., *Elon Musk's Team Now Has Full Access to Treasury's Payments System*, N.Y. TIMES (Feb. 1, 2025).

[3] @wyden.senate.gov, BLUESKY (Feb. 1. 2025, 3:37 PM), https://bsky.app/profile/wyden.senate.gov/post/3lh5ejpwncc23.

2025)) is reported to be working at the Treasury.[4] And Secretary Bessent has reportedly "signed off on a plan to give access to the payment system to a team led by" Mr. Krause, who is identified in the article as "a liaison to Musk's DOGE group that operates out of" the USDS.[5] Defendants have not publicly disclosed the members of Mr. Krause's team or provided the details of the "plan" for access that Secretary Bessent reportedly signed off on. Although an anonymous source assured that "no one outside Treasury would have access" to the payment system, the source apparently did not indicate whether information contained in the payment system would be disseminated outside of the Bureau.

39. Mr. Musk, a private citizen and private company CEO, has suggested that the DOGE team has the unilateral authority to control disbursements at the Bureau. In response to an allegation by General Mike Flynn (ret.) that certain federal grants to Lutheran Family Services and affiliated organizations should end, Mr. Musk responded on X (formerly Twitter) that "The @DOGE team is rapidly shutting down these illegal payments."[6]

40. Moreover, Musk, seemingly confused on the functions of BFS, further emphasized his intentions to stop certain payments by alleging the longtime civil servants at the Bureau of Fiscal Service were criminals. Musk contended "Career

---

[4] Andrew Duehren et al., *Treasury Official Quits After Resisting Musk's Requests on Payments*, N.Y. TIMES (Jan. 31, 2025).

[5] Michael Stratford et al., *Trump administration gives Musk allies access to Treasury payment system*, POLITICO (Feb. 1, 2025).

[6] @elonmusk, X (Feb. 2, 2025, 3:14 AM), https://x.com/elonmusk/status/1885964969335808217.

Treasury officials are breaking the law every hour of every day by approving payments that are fraudulent or do not match the funding laws passed by Congress. This needs to stop NOW!"[7]

41. Notably, BFS does not independently make eligibility determinations of payments. 31 U.S.C § 3325 authorizes the Treasury to disburse payments after it has been properly certified. Therefore, Musk and his DOGE team gaining access to highly sensitive private information becomes more alarming and clearer of the security risk.

42. Mr. Musk was labeled a "special government employee" by the White House. An employee of this nature is authorized to work for the government for only "130 days or less in a 365-day period."[8]

43. The Treasury Order 105-19 states that delegated officials are required to "[e]nsure that personnel in that official's organization with a security clearance for access to classified information are proficient with processing, marking, and safeguarding requirements for classified information."[9]

44. The systems Musk and his DOGE team accessed are subject to strict access and logging requirements. Individuals who do not possess the credentials

---

[7] @elonmusk, X (Feb. 2, 2025, 2:27 PM), https://x.com/elonmusk/status/1886134485822922785

[8] U.S. DEP'T OF JUST., JUST. MGMT. DIV., *Summary of Government Ethics Rules for Special Government Employees* (Feb. 6, 2006), https://www.justice.gov/jmd/ethics/summary-government-ethics-rules-special-government-employees (last visited Feb. 12, 2025).

[9] U.S. DEP'T OF TREAS., *Treasury Order 105-19* (June 27, 2011), https://home.treasury.gov/about/general-information/orders-and-directives/treasury-order-105-19#:~:text=Ensure%20that%20personnel%20in%20that,/or%20bureau%20security%20officials) (last visited Feb. 12, 2025).

needed to access the OPM and Treasury systems have breached the security of those systems.

45. Defendants had a duty to deny access to Defendant Musk and his DOGE employees unless they had the proper credentials or authority. Instead, Defendants permitted a major security breach of highly sensitive private information. Defendants ignored the rule of law and allowed for unwarranted unauthorized access to PSI.

46. Upon information and belief, Musk and his DOGE team did not undergo a proper background check nor receive appropriate security clearances to access the highly sensitive data. Additionally, special government employees are prohibited from using their public office for private gain or that of his or her friends, relatives, or persons whom they are affiliated with.[10] More concerningly, Musk still maintains his role as the CEO of private companies, many of which solicit and accept government contracts.

47. In late January 2025, employees at OPM were instructed to provide information on federal employees to Amanda Scales, a former employee of Elon Musk who, upon information and belief, is acting under Mr. Musk's orders. 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.

48. Upon information and belief, Musk did not undergo the required

[10] 5 C.F.R. § 2635.702; *Summary of Government Ethics Rules for Special Government Employees*, *supra* note 8.

training to access highly confidential files, posing a potential national security risk. Typically, personnel with access to these files receive specialized training to ensure the security of systems containing highly sensitive private information. Such training is also essential to mitigate the risk of threat actors gaining unauthorized access to this data.

49. Scales improperly granted 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.

50. Musk and his DOGE team, without authorization, obtained access to computers maintained by the Department of Education, giving him access to student loan data, including Social Security numbers, dates of birth, and contact information, for millions of federal student loan borrowers.

Defendants' Unlawful Actions Harm the Plaintiffs and Class Members

51. Plaintiffs and the members of the Class are among the millions of people who receive money from the federal government using the Bureau's payment, collections, and electronic funds systems, including monthly Social Security retirement payments from the Treasury, Railroad Retirement Benefits, pension income for federal government service, disability and workers compensation benefits under the Federal Employees' Compensation Program, federal black lung benefits and veterans benefits.

52. Plaintiffs and the members of the Class also pay federal income taxes or

receive refunds and who have done so and will do so again in the current tax season.

53. The Bureau will collect and maintain personal and financial information about Plaintiffs and members of the Class to make the income payments and benefits they are owed and to process their tax payments or refunds.

54. Defendants have the statutory responsibility to protect the sensitive personal and financial information that they collect and maintain about individuals from unnecessary and unlawful disclosure to third parties. Defendants have acted inconsistently with that responsibility by granting individuals associated with DOGE access to the extensive records that the Bureau maintains on every individual with whom it engages in financial transactions. Moreover, Defendants have taken this action without obtaining or even asking for the consent of affected individuals.

55. Plaintiffs and members of the Class rely on Defendants' payment, collection, and other systems to make and receive payments from the government. They do not have the option of avoiding dealing with Defendants to avoid improper disclosure or misuse of their personal and financial information. Defendants' actions have thus harmed Plaintiffs and members of the Class by depriving them of privacy protections guaranteed to them by federal law and, consequently, the ability to decide for themselves whether Elon Musk or other individuals should be able to obtain and use their personal data to advance DOGE's agenda.

56. As a result of Defendants' violations of law, Plaintiffs and Class members have sustained and will continue to sustain economic loss and other harm. They have experienced and/or face an increased risk of experiencing the following

forms of injuries:

A. money expended for purchase costs from the purchase of credit monitoring and identity theft protection services;

B. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of PSI, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards;

C. money and time lost as a result of fraudulent access to and use of their financial accounts, some of which accounts were never reimbursed;

D. loss of use of and access to their financial accounts and/or credit;

E. diminished prospects for future employment and/or promotion to positions with higher security clearances as a result of their PSI having been compromised;

F. money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;

G. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

H. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

I. money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns, including by completing paperwork associated with the reporting of fraudulent returns and the manual filing of replacement returns;

J. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches, including efforts to research how to prevent, detect, contest, and recover from misuse of PSI;

K. loss of the opportunity to control how their PSI is used;

L. continuing risks from the unmasking of confidential identities; and

M. continuing risks to their PSI and that of their family members, friends, and associates, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the PSI in its possession.

CLASS ACTION ALLEGATIONS

57. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), and/or (b)(1), (b)(2), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

58. The proposed Class is defined as:

> All persons in the United States who receive payments from or submitted payments to the United States government and their family members and cohabitants, and whose Personal Sensitive Information ("PSI") was accessed without their prior written authorization from the OPM or the Department of Treasury beginning in January 2025.

Excluded from the proposed Class and Subclass are:

A. Senior officers, officials, and executives of Defendants and their immediate family members; and

B. Any judicial officers to whom this case is assigned and their respective staffs.

Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into further subclasses, or modified in any other way.

Numerosity and Ascertainability

59. The size of the Class cannot be estimated with reasonable precision, but it likely in the tens of millions. The number is great enough that joinder is impracticable. The disposition of their claims in a single action will provide substantial benefits to all parties and to the Court.

60. Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants. Notice of this action can be readily provided to the Class.

Typicality

61. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised in the Data Breaches.

Adequacy of Representation

62. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class members.

Predominance of Common Issues

63. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

A. Whether Defendants, in violation of the Privacy Act, disclosed Plaintiffs' and Class members' PSI without their prior written consent for no statutorily permitted purpose;

B. Whether Defendants' conduct violated the Administrative Procedure Act and, if so, what equitable remedies should issue;

C. Whether Plaintiffs and Class members are entitled to damages and declaratory and injunctive relief.

Superiority

64. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class members' claims, it is likely that few, if any, Class members could afford to seek redress for Defendants' violations.

65. Class treatment of common questions of law and fact would also be a superior method to piecemeal litigation in that class treatment will conserve the resources of the courts and will promote consistency and efficiency of adjudication.

66. Class-wide declaratory, equitable, and injunctive relief is appropriate under Rule 23(b)(1), (b)(2), and/or (c)(4) because Defendants have acted on grounds that apply generally to the Class, and inconsistent adjudications would establish incompatible standards and substantially impair the ability of Class members and Defendants to protect their respective interests. Class-wide relief assures fair, consistent, and equitable treatment of Class members and Defendants.

CAUSES OF ACTION

COUNT ONE
Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)
(against Defendant Elon Musk)

67. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

68. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, prohibits unauthorized access to protected computers with the intent to defraud and obtain

anything of value.

69. Defendant Musk knowingly and intentionally accessed a protected computer without authorization or exceeded authorized access, in violation of 18 U.S.C. § 1030(a)(2).

70. Defendant Musk knowingly and intentionally obtained information from a department or agency of the United States or from a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(B) & (C).

71. Specifically, as alleged herein, on or about January 31, 2025, Defendant Musk, a private citizen, was given full access to the Bureau's data and the computer systems that house them by Defendant Bessent, without authorization of law.

72. Specifically, as alleged herein, on or about January 31, 2025, OPM illegally and improperly violated the restrictions on disclosure of PSI by giving full access to OPM's data and the computer systems that house them to Defendant Musk without a lawful or legitimate need for such data and without him having undergone the security clearance process.

73. The computers accessed by Defendant Musk qualify as protected computers under 18 U.S.C. § 1030(e)(2), as they are used in or affect interstate or foreign commerce and communication.

74. As a direct and proximate result of Defendant Musk's actions, Plaintiffs and the Class members have suffered damages and losses, as alleged herein, and including, without limitations, the cost of credit monitoring and identify protection services, in an amount to be proven at trial, but in no event less than $5,000

aggregated over a one-year period across all Plaintiffs and Class members, as required by 18 U.S.C. § 1030(c)(4)(A)(i)(I).

75. The losses suffered by Plaintiffs and Class members include the cost of responding to the offense, including, without limitation, credit monitoring and identity protection services and lost time responding to data abuse subsequent to the Data Breaches set forth herein.

76. Plaintiffs are entitled to compensatory damages and injunctive relief or other equitable relief under 18 U.S.C. § 1030(g).

COUNT TWO
Violation of the Privacy Act of 1974, 5 U.S.C. § 552a
(against Defendants OPM and Treasury)

77. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

78. OPM and the Treasury are agencies within the meaning of the Privacy Act.

79. 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."

80. 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."

81. Defendants obtained and preserved Plaintiffs' and Class members' PSI in a system of records during the recruiting and security check processes.

82. Defendants 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)."

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

84. 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 to comply with FISMA.

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

A. 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);

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).

74. Through a continuous course of conduct, OPM and Treasury 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's and the Treasury Department's 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.

75. 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.

76. 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 as set forth herein.

77. 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 seek a judgment against Defendants through an Order:

A. certifying this case as a class action, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel to represent the Class;

B. finding Defendants liable for their willful failure to ensure the security of Plaintiffs' and Class members' PSI;

C. requiring Defendants to pay money damages, including actual and statutory damages, to Plaintiffs and Class members;

D. declaring that the relevant conduct of Defendants is unlawful, and that Defendants shall indemnify and hold harmless any Class member who has sustained or will sustain economic injury as a result of the Data Breaches;

E. enjoining Defendant Musk from further violations of the CFAA;

F. enjoining Defendants to extend free lifetime identity theft and fraud protection services, including credit monitoring and identity theft insurance, to Plaintiffs and the Class;

G. awarding reasonable attorneys' fees and costs as may be permitted by law;

H. awarding pre-judgment and post-judgment interest as may be prescribed by law; and

I. granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: February 12, 2025

Respectfully submitted,

/s/ Gary E. Mason

Gary E. Mason (DC Bar No. 418073)
Danielle L. Perry (DC Bar No. 1034960)
Salena J. Chowdhury (DC Bar No. 90010584)
MASON LLP
5335 Wisconsin Avenue NW
Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: schowdhury@masonllp.com

Attorneys for Plaintiffs