IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

ELECTRONIC PRIVACY INFORMATION CENTER;
1519 New Hampshire Avenue, N.W.
Washington, D.C. 20036

DOE 1

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT
1900 E Street NW
Washington, D.C. 20415

Case No. _____

CHARLES EZELL, in his official capacity as Acting Director of the Office of Personnel Management
1900 E Street NW
Washington, D.C. 20415

U.S. DEPARTMENT OF THE TREASURY
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

SCOTT BESSENT, in his official capacity as Secretary of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

U.S. DOGE SERVICE;
736 Jackson Place NW
Washington, D.C. 20503

ACTING U.S. DOGE ADMINISTRATOR
736 Jackson Place NW
Washington, D.C. 20503

U.S. DOGE SERVICE TEMPORARY ORGANIZATION
736 Jackson Place NW
Washington, D.C. 20503

Defendants.

COMPLAINT FOR DAMAGES, INJUNCTIVE, MANDAMUS, AND DECLARATORY RELIEF

1. This action arises from the largest and most consequential data breach in U.S. history, currently ongoing at the U.S. Department of the Treasury and U.S. Office of Personnel Management. This unprecedented breach of privacy and security implicates the personal information of tens of millions of people, including nearly all federal employees and millions of members of the American public.

2. Acting in concert with Defendants U.S. Digital Service ("USDS"), the unidentified Acting Director of the USDS, and the U.S. DOGE Service Temporary Organization ("USDSTO"), Defendants Office of Personnel Management ("OPM"); Charles Ezell, in his official capacity as Acting Director of OPM; the Department of the Treasury ("Treasury"); and Scott Bessent, in his official capacity as Secretary of the Treasury, have allowed the unlawful misuse of critical data systems housed in OPM and the Treasury Department, endangering plaintiffs and millions of other Americans. Defendants Treasury and Bessent (collectively "Treasury Defendants") and Defendants OPM and Acting OPM Director Ezell (collectively "OPM Defendants") have manifestly failed to provide and abide by legally required safeguards to protect the information within their systems.

3. Treasury Defendants and OPM Defendants (collectively "Government Defendants") have deliberately provided Defendants U.S. Digital Service ("USDS"), the unidentified Acting Director of the USDS, and the U.S. DOGE Service Temporary Organization ("USDSTO") (collectively "DOGE Defendants") with unlawful access to sensitive and protected data, and have allowed that data to be used for legally prohibited purposes. These basic security failures have resulted in the unlawful disclosure of personal data—including social security

numbers and tax information—belonging to tens of millions of individuals stored in Bureau of Fiscal Service ("BFS") systems and the unlawful disclosure of personal data belonging to millions of federal employees stored in Enterprise Human Resources Integration ("EHRI").

4. DOGE Defendants have exceeded the scope of their legal authority by accessing and controlling OPM and Treasury systems. These *ultra vires* actions have resulted in unlawful disclosure of the contents of these systems, violated Plaintiffs' constitutional right to privacy of information, and endangered the security of the information they contain.

5. Plaintiffs seek injunctive relief curing Government Defendants' unlawful failure to secure personal information contained in the EHRI system and BFS payment systems; halting all Defendants' unlawful use of such systems for impermissible purposes and without required information security safeguards; and halting the unlawful disclosure and computer matching of sensitive personal information. Plaintiffs seek injunctive and/or mandamus relief halting the DOGE Defendants' unlawful, *ultra vires* direction of the use and administration of the EHRI system and BFS payment systems.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, 5 U.S.C. § 704, 5 U.S.C. § 552a(g)(5), 26 U.S.C. § 7431(a)(1), and 28 U.S.C. § 1361.

7. Venue is proper in this district because Plaintiff Doe 1 resides in this District. 28 U.S.C. § 1391(e)(1).

8. Venue is proper in the Alexandria division because Plaintiff Doe 1 resides within the Alexandria division as described in Local Rule 3(B)(1).

PARTIES

9. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities that impact individual privacy. EPIC is a membership organization. An individual member of EPIC is any person who contributes to the advancement of the mission of EPIC, who acts in accordance with the core values and policies of EPIC, and who has been recognized and registered as a member by EPIC, by virtue of payment of annual dues or having been granted a dues waiver. This includes members of EPIC's Advisory Board, who are distinguished experts in law, technology, and public policy.

10. Doe 1 is a current federal employee of an agency subject to U.S. Code Title 5.

11. Defendant U.S. Office of Personnel Management is an agency within the meaning of 5 U.S.C. § 701(b)(1), 5 U.S.C. § 552a(a)(1), and 5 U.S.C. § 552(f).

12. Defendant Charles Ezell is the Acting Director of the U.S. Office of Personnel Management and an officer or employee of the United States within the meaning of 26 U.S.C. § 7431. He is sued in his official capacity.

13. Defendant U.S. Department of the Treasury is an agency within the meaning of 5 U.S.C. § 701(b)(1), 5 U.S.C. § 552a(a)(1), and 5 U.S.C. § 552(f).

14. Defendant Scott Bessent is the Secretary of the Treasury and an officer or employee of the United States within the meaning of 26 U.S.C. § 7431. He is sued in his official capacity.

15. Defendant U.S. Digital Service, also known as the United States DOGE Service, is a subcomponent of the Executive Office of the President and an agency within the meaning of 5 U.S.C. § 701(b)(1).

16. Defendant Acting U.S. Digital Service Administrator is the head of the USDS.

17. Defendant U.S. DOGE Service Temporary Organization is a subcomponent of the USDS, a subcomponent of the Executive Office of the President, and an agency within the meaning of 5 U.S.C. § 701(b)(1).

Legal Framework

18. Government information systems are subject to comprehensive privacy and information security protections.

19. The Federal Information Security Modernization Act of 2014 ("FISMA"), 44 U.S.C. §§ 3551–58, requires agencies to provide information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized access [or] use" of information or information systems maintained by the agency, *id.* § 3554(a)(1)(A).

20. The Privacy Act of 1974, 5 U.S.C. § 552a, prohibits disclosure of information from systems of records except in enumerated circumstances.

21. The Privacy Act further requires that, when an agency establishes or revises a system of records, it must issue a System of Records Notice (SORN), which discloses information about the records in the system, the manners in which those records may be used, and storage and access policies. 5 U.S.C. § 552a(e)(4).

22. The E-Government Act of 2002, Pub. L. 107-347, requires that agencies conduct a privacy impact assessment for new or substantially changed information technology which contains certain records. Privacy act assessments are intended to "demonstrate that system

owners and developers have incorporated privacy protections throughout the entire life cycle of a system." *E-Government Act of 2002*, Department of Justice: Office of Privacy and Civil Liberties, https://www.justice.gov/opcl/e-government-act-2002.

23. Federal agencies are also subject to standards and guidance developed by the National Institute of Standards and Technology ("NIST"). NIST develops and implements "standards to be used by all agencies to categorize all information and information systems" in order to "provid[e] appropriate levels of information security according to a range of risk levels" and "minimum information security requirements for information and information systems." 15 U.S.C. § 278g–3(b)(1). The Secretary of Commerce is further empowered to make those standards "compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems." 40 U.S.C. § 11331.

24. Those mandatory standards for Federal information systems can be found in NIST Special Publication 800-53. NIST SP-800-53, *Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce: National Institute of Standards and Technology (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. The standards require that when federal agencies process personally identifiable information, they must abide by information security and privacy programs designed to manage the security risks for the PII in the system. *Id.* at 13.

25. The Internal Revenue Code, 26 U.S.C. § 6103, provides that "[r]eturns and return information shall be confidential" and prohibits the disclosure and use of this information by United States employees and other defined persons, except as specifically authorized by statute. This protection is an essential component of the due process granted to taxpayers by the

Government. Indeed, the IRS has made the right of confidentiality core to its "The Taxpayer Bill of Rights." This "general ban on disclosure provides essential protection for the taxpayer; it guarantees that the sometimes sensitive or otherwise personal information in a return will be guarded from persons not directly engaged in processing or inspecting the return for tax administration purposes. The assurance of privacy secured by § 6103 is fundamental to a tax system that relies upon self-reporting." *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000).

26. Taxpayers have a private right of action to seek damages under 26 U.S.C. § 7431 for the knowing or negligent unauthorized inspection or disclosure of returns or return information in violation of 26 U.S.C. § 6103.

27. The term "disclosure" means "the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8).

28. The term "return" is broadly defined to include "any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed." 26 U.S.C. 6103(b)(1).

29. Records of tax payments and tax deposits are tax return information under 26 U.S.C. § 6103.

FACTS

The Establishment of the "Department of Government Efficiency"

30. On November 12, 2024, then-President-Elect Trump announced the creation of the "Department of Government Efficiency" ("DOGE"). At the time, President-Elect Trump said that DOGE would not be a formal part of the government. Instead, DOGE was to be created to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget," to "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[1]

31. In the time between the election and President Trump's inauguration, DOGE personnel spoke with staffers at federal agencies including the Department of Treasury, the Internal Revenue Service, the Department of Homeland Security, Veterans Affairs, and the U.S. Department of Health and Human Services.[2] They were directed in large part by Elon Musk, an individual who is either the Acting USDS Administrator or otherwise exercising substantial authority within USDS.

32. On the day of his inauguration, January 20, 2025, President Trump signed Executive Order 14158, Establishing and Implementing the President's "Department of Government Efficiency," ("the E.O."), reorganizing and renaming the United States Digital

[1] *See* Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, 7:46 PM ET), https://truthsocial.com/@realDonaldTrump/posts/113472884874740859.
[2] Faiz Siddiqui, Jeff Stein and Elizabeth Dwoskin, *DOGE is dispatching agents across U.S. government*, Wash. Post (Jan. 10, 2025), https://www.washingtonpost.com/business/2025/01/10/musk-ramaswamy-doge-federal-agencies/.

Service as the United States DOGE Service, established in the Executive Office of the President.[3]

33. The E.O. established the role of U.S. DOGE Service Administrator in the Executive Office of the President, reporting to the White House Chief of Staff.[4]

34. The E.O. further established within U.S. DOGE Service a temporary organization known as "the U.S. DOGE Service Temporary Organization." The U.S. DOGE Service Temporary Organization is headed by the U.S. DOGE Service Administrator and is tasked with advancing "the President's 18-month DOGE agenda."[5]

35. The E.O. also requires each Agency Head to establish a "DOGE Team" comprised of at least four employees within their respective agencies. DOGE Teams are required to "coordinate their work with [U.S. DOGE Service] and advise their respective Agency Heads on implementing the President's DOGE Agenda."[6]

36. The E.O. instructed the U.S. DOGE Service Administrator to "commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems."[7] The Administrator must work with Agency Heads to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization."[8]

37. The E.O. further requires Agency Heads to take all necessary steps "to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT

[3] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025).
[4] *Id.* at § 3(b).
[5] *Id.*
[6] *Id.* at § 3(c).
[7] *Id.* at § 4(a).
[8] *Id.*

systems."[9] The E.O. nominally directs the U.S. DOGE Service to adhere to "rigorous data protection standards."[10]

The Seizure, Breach, and Misuse of Key Federal Information Systems

38. Since Inauguration Day, USDS/DOGE personnel, many of them associates of Elon Musk, have sought and obtained unprecedented access to information systems across numerous federal agencies, including the Department of Treasury and the Office of Personnel Management.[11]

39. Under normal circumstances, these systems and the information contained therein are carefully protected by, *inter alia*, rigorous information security protocols mandated by FISMA, robust privacy protections established by the Privacy Act of 1974, and careful supervision by trained agency personnel.

40. Yet at the direction and insistence of DOGE Defendants, Government Defendants have abandoned these safeguards, relinquishing control of these systems and, without legal basis, disclosing vast stores of personal information to individuals unauthorized by law to access them, including but not limited to USDS/DOGE personnel.

41. Individuals affiliated with or acting at the urging of USDS/DOGE have also connected hard drives and at least one server to these critical systems. On information and belief, these devices are not compliant with FISMA or other applicable privacy and security requirements, introducing substantial vulnerabilities to these systems.

---

[9] *Id.* at 4(b).
[10] *Id.*
[11] Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, The Washington Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/.

Treasury Department/Bureau of the Fiscal Service Payment Systems

42. Treasury houses the Bureau of the Fiscal Service ("BFS"), which controls a federal payment system that distributes nearly 90% of all federal payments, including Social Security benefits, tax refunds, and vendor payments.[12] BFS payment systems process more than $6 trillion in annual payments and are responsible for more than a billion payments annually.[13]

43. BFS payment systems contain vast amounts of sensitive personal data of tens of millions of individuals. As one example, the BFS's Integrated Document Management System ("IDMS") contains personally identifying information for "10,000,000–99,999,999" individuals, including Social Security Numbers, personal taxpayer identification numbers, personal financial information, taxpayer information/return information, dates of birth, addresses, zip codes, phone numbers, email addresses, marital statuses, spouse information, information on children, mother's maiden names, military service information, employee identification numbers, health plan beneficiary numbers, patient ID numbers, file/case ID numbers, medical/health information, mental health information, worker's compensation information, disability information, and emergency contact information.[14]

---

[12] Katelyn Polantz, Phil Mattingly & Tierney Sneed, *How an Arcane Treasury Department Office Is Now Ground Zero in the War over Federal Spending*, CNN (Feb. 1, 2025), https://www.cnn.com/2025/01/31/politics/doge-treasury-department-federal-spending/index.html.

[13] Letter from U.S. Sen. Ron Wyden to Treasury Secretary Scott Bessent (Jan. 31, 2025), https://www.finance.senate.gov/imo/media/doc/letter_from_senator_wyden_to_secretary_bessent_on_payment_systemspdf.pdf.

[14] BSF, Privacy and Civil Liberties Impact Assessment, *Integrated Document Management System-Records Management (IDMS-RM*), 11 (Oct. 8, 2019), https://www.fiscal.treasury.gov/files/pia/IDMS-pia.pdf [https://perma.cc/Q3V5-AVYE].

44. Across presidential administrations of both parties, including President Trump's first administration, BFS systems have historically—and successfully—been operated by career civil servants without direct involvement by political employees.

45. Individuals' full Social Security Numbers—among the most sensitive and carefully guarded categories of personal data—are housed across numerous BFS systems, including the IDMS,[15] the Disbursement And Debt Management Analytics Platform,[16] Do Not Pay,[17] the Electronic Check Processing System,[18] the Electronic Federal Tax Payments System,[19] FedDebt,[20] the Fiscal Data Hub,[21] the Invoice Processing Platform,[22] the Payment Information Repository,[23] Payment Information & View of Transactions,[24] the Secure Payment System,[25] the

[15] *Id.*
[16] Privacy and Civil Liberties Impact Assessment, *Disbursement And Debt Management Analytics Platform (DDMAP)*, BSF, 7 (Mar. 17, 2023), https://www.fiscal.treasury.gov/files/pia/ddmap-pclia.pdf.
[17] Privacy and Civil Liberties Impact Assessment, *Do Not Pay*, BSF, 7 (July 14, 2024), *https://www.fiscal.treasury.gov/files/pia/dnp-pclia.pdf.*
[18] Privacy and Civil Liberties Impact Assessment, *Electronic Check Processing (ECP) System*, BSF, 6 (Aug. 23, 2024), https://www.fiscal.treasury.gov/files/pia/ecp-pclia.pdf.
[19] Privacy and Civil Liberties Impact Assessment, *Electronic Federal Tax Payments System (EFTPS)*, BSF, 7 (June 6, 2024), https://www.fiscal.treasury.gov/files/pia/eftps-pia.pdf.
[20] Privacy and Civil Liberties Impact Assessment, *FedDebt*, BSF, 7 (June 6, 2023) https://www.fiscal.treasury.gov/files/pia/feddebt-pclia.pdf.
[21] Privacy and Civil Liberties Impact Assessment, *Fiscal Data Hub (DH)*, BSF, 7 (Sept. 19, 2023) https://www.fiscal.treasury.gov/files/pia/fiscal-data-hub-pclia.pdf.
[22] Privacy and Civil Liberties Impact Assessment, *Invoice Processing Platform (IPP)*, BSF, 7 (Feb. 15, 2024), https://www.fiscal.treasury.gov/files/pia/IPP-pclia.pdf.
[23] Privacy and Civil Liberties Impact Assessment, *Payment Information Repository (PIR)*, BSF, 11 (Apr. 6, 2020), https://www.fiscal.treasury.gov/files/pia/pir-pclia.pdf.
[24] Privacy and Civil Liberties Impact Assessment, *Payment Information & View of Transactions (PIVOT)*, BSF, 7 (May 4, 2022), https://www.fiscal.treasury.gov/files/pia/pivot-pclia.pdf.
[25] Privacy and Civil Liberties Impact Assessment, *Secure Payment System (SPS)*, BSF, 7 (Mar. 22, 2021), https://www.fiscal.treasury.gov/files/pia/spspclia.pdf.

Treasury Check Information System,[26] and Treasury Direct.[27] Pursuant to the Federal Information Security Modernization Act, at least some of these systems are designated high security,[28] meaning that unauthorized disclosures, modifications, or disruptions to access of the systems could have "severe or catastrophic adverse effect[s] on organizational operations, organizational assets, or individuals."[29]

46. Along with the other robust protections that ensure the security of this information, the data on BFS systems are subject to Privacy Act system of records notices (SORNs). These SORNs establish that personal information contained in BFS systems is to be disclosed only for narrow, carefully defined purposes relating or incident to the accounting, payment processing, and public debt responsibilities of the BFS.[30]

47. These purposes do not include dismantling, slashing, and restructuring federal programs.

48. Over the past week, the Treasury Department has flagrantly violated these safeguards at the direction and insistence of the USDS/DOGE.

---

[26] Privacy and Civil Liberties Impact Assessment, *Treasury Check Information System (TCIS)*, BSF, 12 (Apr. 16, 2020), https://www.fiscal.treasury.gov/files/pia/tcis-pclia.pdf.
[27] Privacy and Civil Liberties Impact Assessment, *TreasuryDirect (TD)*, BSF, 7 (Dec. 19, 2023), https://www.fiscal.treasury.gov/files/pia/treasurydirect-pclia.pdf.
[28] *See*, *e.g.*, GovTribe.com, *Secure Payment System O & M Support Services* (May 11, 2022), https://govtribe.com/opportunity/federal-contract-opportunity/secure-payment-system-o-m-support-services-rfifsa23001.
[29] *Standards for Security Categorization of Federal Information and Information Systems*, U.S. Dep't of Comm., FIPS PUB 199 1, 6 (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.
[30] System of Records, 85 Fed. Reg. 11,776 (Feb. 27, 2020), https://www.federalregister.gov/documents/2020/02/27/2020-03969/privacy-act-of-1974-system-of-records.

49. On Inauguration Day, January 20, 2025, Trump named David Lebryk, a nonpolitical career civil servant who has spent 35 years in government service,[31] as acting Secretary of the Treasury.[32]

50. DOGE personnel asked Lebryk about Treasury's ability to stop payments, to which Lebryk responded, "We don't do that."[33]

51. A week later, on January 27, 2025, Defendant Scott Bessent was confirmed as Secretary of the Treasury.[34]

52. Sometime between January 27 and January 31, Lebryk was placed on administrative leave because he had resisted requests to access BFS payment systems from DOGE personnel.[35]

---

[31] *David Lebryk*, U.S. Dept. of the Treasury, https://home.treasury.gov/about/general-information/officials/david-lebryk; Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/.

[32] Press Release, *President Trump Announces Acting Cabinet and Cabinet-Level Positions*, The White House (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/designation-of-acting-leaders/.

[33] Katelyn Polantz, Phil Mattingly & Tierney Sneed, *How an Arcane Treasury Department Office Is Now Ground Zero in the War over Federal Spending*, CNN (Feb. 1, 2025), https://www.cnn.com/2025/01/31/politics/doge-treasury-department-federal-spending/index.html.

[34] Fatima Hussein, *Scott Bressent Confirmed as Treasury Secretary, Giving Him a Key Role in Extending Trump's Tax Cuts*, AP (Jan. 27, 2025), https://apnews.com/article/bessent-confirmed-treasury-secretary-2ca8eb1c882d094b032584adf1a95c48.

[35] Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/; Andrew Duehren et al., *Treasury Official Quits After Resisting Musk's Requests on Payments*, N.Y. Times (Jan. 31, 2025), https://www.nytimes.com/2025/01/31/us/politics/david-lebryk-treasury-resigns-musk.html.

53. Lebryk subsequently announced his retirement in a January 31, 2025, email to Treasury colleagues.[36]

54. Career Treasury employees have consistently underscored to DOGE affiliates that it is not the role of Treasury or BFS to approve or deny payments because "the decision about whether to approve or deny payments belongs to individual agencies based on funds appropriated by Congress."[37]

55. Late on January 27, 2025, Secretary Bessent granted USDS/DOGE personnel access to the BFS's payment systems.[38]

56. Anyone with access to these Treasury payment systems—now including at least some DOGE operatives—can stop payments from the federal government, including the ability to "turn off funding selectively."[39]

57. By granting BFS payment system access to USDS/DOGE, Secretary Bessent and the Treasury Department disclosed vast stores of personal information contained in those systems to individuals not authorized by law to access them.

---

[36] Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/.

[37] Gregory Korte & Viktoria Dendrinou, *Musk Says DOGE Halting Treasury Payments to US Contractors*, Bloomberg (Feb. 2, 2025), https://www.bloomberg.com/news/articles/2025-02-02/musk-says-doge-is-rapidly-shutting-down-treasury-payments.

[38] Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payment System*, N.Y. Times (Feb. 1, 2025), https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html; Jeff Stein, *Musk Aides Gain Access to Sensitive Treasury Department Payment System*, Wash. Post (Feb. 1, 2025), https://www.washingtonpost.com/business/2025/02/01/elon-musk-treasury-payments-system/.

[39] Greg Sargent, *Trump and Elon Musk Just Pulled off Another Purge – And It's a Scary One*, The New Republic (Jan. 31, 2025), https://newrepublic.com/article/191014/trump-elon-musk-treasury-purge.

58. At least one former employee of Elon Musk, Marko Elez, was granted administrator-level privileges over BFS payment systems, including but not limited to the Payment Automation Manager, the Secure Payment System (SPS), and the Electronic Federal Tax Payments System.[40]

59. Administrative privileges granted Elez power to "navigate an entire file system, change user permissions, . . . delete or modify critical files . . . bypass the security measures of, and potentially cause irreversible changes to, the very systems they have access to."[41]

60. Federal information technology experts have stated that nobody would need these privileges to hunt down fraudulent payments or to analyze the disbursement of funds.[42] A source reported they were concerned that data could be passed from the Payment Automation Management and Secure Payment System to DOGE personnel embedded in other agencies.[43]

61. Elez's access was unlawful under the Privacy Act and in violation of established security policies and requirements. On information and belief, Elez lacked requisite training in the handling of sensitive personal data.

62. That access is also unnecessary; Elez had no lawful reason to have access to these systems.

---

[40] James Lidell, *A 25-year-old Elon Musk acolyte has access to 'nearly all payments made by U.S. government'*, The Independent (Feb. 4, 2025), https://www.the-independent.com/news/world/americas/us-politics/elon-musk-marko-elez-treasury-doge-b2691932.html

[41] *A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System*, WIRED (Feb. 4, 2025) https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/

[42] *Id.*

[43] *Id.*

63. Elez has since resigned from DOGE.[44]

64. Unsurprisingly, within a day of this unlawful and unprecedented provision of access and disclosure of personal data, information exfiltrated from the BFS payment systems was broadcast to a wide audience on Twitter/X.

65. Specifically, on February 1, 2025, a post by retired Lt. Gen. Mike Flynn disclosed screenshots showing 42 payments from the Department of Health and Human Services to various recipients.[45] Flynn specifically criticized payments to Lutheran Family Services, "a faith-based charity that has been providing social services to refugees," in his tweet.[46]

66. The screenshots in Mr. Flynn's tweet disclosed the award ID, date, total amount, and recipient for each of the 42 payment entries.[47] Mr. Flynn's tweet added: "And there is much more where these screen shots below came from."[48]

67. On information and belief, the information contained in Mr. Flynn's tweet was taken from protected BFS systems.

68. Elon Musk replied to this tweet on his personal Twitter/X account: "The @DOGE team is rapidly shutting down these illegal payments."[49]

---

[44] *The US Treasury Claimed DOGE Technologist Didn't Have "Write Access" When He Actually Did*, WIRED (Feb. 6, 2025).
[45] Mike Flynn (@GenFlynn), Twitter/X (Feb. 1, 2025, 9:04 PM ET), https://x.com/GenFlynn/status/1885872007062892568.
[46] *Id.*; Gregory Korte &Viktoria Dendrinou, *Musk Says DOGE Halting Treasury Payments to US Contractors*; Bloomberg (Feb. 2, 2025), https://www.bloomberg.com/news/articles/2025-02-02/musk-says-doge-is-rapidly-shutting-down-treasury-payments.
[47] *Id.*
[48] *Id.*
[49] Elon Musk (@elonmusk), Twitter/X (Feb. 2, 2025, 3:14 AM ET), https://x.com/elonmusk/status/1885964969335808217.

69. After USDS/DOGE personnel were granted access to Treasury payment systems, the official DOGE account on Twitter/X tweeted that it was "stopping improper payments."[50]

70. On the basis of these public messages, and upon further information and belief, USDS/DOGE and Treasury Department personnel are unlawfully exfiltrating identifying information from BFS payment systems, impermissibly matching this information with other data sets, and using and redisclosing such information for impermissible purposes.

71. For example, the privacy impact assessments for SPS and other BFS payment systems state that personal information maintained within the systems will not be used as part of a matching program.[51]

72. On information and belief, USDS/DOGE operatives are using personal information from these systems to conduct computer matching of personal information.

73. The privacy impact assessments for SPS and other accessed BFS payment systems state that personal information maintained in the system is not shared with agencies, organizations, or individuals external to the Treasury.[52]

74. On information and belief, Treasury has shared personal information with individuals not employed at Treasury, including USDS/DOGE personnel.

75. The privacy impact assessments for multiple Treasury payment systems designed to facilitate payments and deliver government benefits and services state the personal

[50] Department of Government Efficiency (@DOGE), Twitter/X (Jan. 28, 2025, 7:20 PM ET), https://x.com/DOGE/status/1884396041786524032.
[51] *See e.g.*, Privacy and Civil Liberties Impact Assessment, Secure Payment System (SPS), Mar. 22, 2021, https://www.fiscal.treasury.gov/files/pia/spspclia.pdf 13.
[52] *Id*. at 14.

information in such systems shall not be "used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs."[53]

76. On information and belief, the Treasury, at the direction of USDS/DOGE, is moving to stop approved payments to federal contractors, charities that provide social services, and other federal departments. The USDS/DOGE has further indicated that it is likely to target vital public benefits programs.

The Office of Personnel Management's EHRI System

77. OPM hosts and administers the Enterprise Human Resources Integration, which is "responsible for maintaining the integrity of the electronic Official Personnel Folder (eOPF), which protects information rights, benefits, and entitlements of federal employees."

78. The EHRI Data Warehouse, a component of the EHRI, "is the Federal government's source for integrated Federal workforce information and includes career lifecycle information that encompasses human resource data, training data, and payroll data."[54]

79. The "system currently collects, integrates, and publishes data for 2.0 million Executive Branch employees on a bi-weekly basis, supporting agency and governmentwide analytics."[55]

---

[53] *See e.g.*, *id.* at 11.
[54] *Privacy Impact Assessment for Enterprise Human Resources Integration Data Warehouse*, U.S. Office of Personnel Management (July 11, 2019) https://www.opm.gov/information-management/privacy-policy/privacy-policy/ehridw.pdf
[55] *Enterprise Human Resources Integration: Data Warehouse*, U.S. Office of Personnel Management, https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human-resources-integration/#url=Data-Warehouse.

80. "Contained within the EHRI are the Social Security numbers, dates of birth, salaries, home addresses, and job descriptions of all civil government workers, along with any disciplinary actions they have faced."[56]

81. Pursuant to FISMA, EHRI is categorized as a high risk information system, for which "the unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals," and "[t]he disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."[57]

82. Like the BFS systems, information in EHRI is protected by a robust set of legal safeguards, including SORNs.

83. The principal SORN applicable to EHRI makes clear that personal information contained in EHRI is to be disclosed only for narrow, carefully defined purposes relating or incident to the provision of human resource services. These purposes do not include dismantling, slashing, and restructuring federal programs.

84. Over the past two weeks, OPM has flagrantly violated these safeguards at the direction and insistence of the USDS/DOGE.

---

[56] Caleb Ecarma and Judd Legum, *Musk associates given unfettered access to private data of government employees*, MuskWatch (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered.

[57] *See Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse*, U.S. Office of Personnel Management Office of the Inspector General, Rep. No. 4A-CI-00-19-006 1, 6 (2019), https://www.oversight.gov/sites/default/files/documents/reports/2022-01/4a-ci-00-19-006.pdf; FIPS PUB 199, *supra* n. 29 at 6.

85. On January 20, 2025, Inauguration Day, Musk and others affiliated with DOGE "assumed command" of OPM by taking over the agency's headquarters, which can only be accessed with a security badge or security escort.[58] OPM employees described the move as a "hostile takeover."[59]

86. USDS/DOGE personnel took control of computer systems, and at least six DOGE agents were given broad access to all personnel systems, including the EHRI system.[60] USDS/DOGE Personnel then locked career civil servants at OPM out of those same systems.[61]

87. According to two OPM staffers, the USDS/DOGE personnel now have "the ability to extract information from databases that store medical histories, personally identifiable information, workplace evaluations, and other private data."[62] That includes personal information for the 24.5 million people who applied for federal employment on USAJobs.[63]

88. USDS/DOGE personnel emailed an OPM staffer, directing the staffer to give USDS/DOGE access "as an admin user" to the system and "code read and write permissions."[64]

---

[58] Tim Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, Reuters (Feb. 1, 2025), https://www.reuters.com/world/us/senior-us-treasury-official-david-lebryk-leave-agency-soon-wapo-reports-2025-01-31/.
[59] *Id.*
[60] Isaac Stanley-Becker, et al., *Musk's DOGE agents access sensitive personnel data, alarming security officials*, Wash. Post (Feb. 6, 2025) https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/.
[61] Tim Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, Reuters (Feb. 1, 2025), https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.
[62] Caleb Ecarma & Judd Legum, *Musk Associates Given Unfettered Access to Private Data of Government Employees*, Musk Watch (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered.
[63] Isaac Stanley-Becker, et al., *Musk's DOGE agents access sensitive personnel data, alarming security officials*, Wash. Post (Feb. 6, 2025) https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/.
[64] *Id.*

The staffer said that level of permission would allow USDS/DOGE to "make updates to anything that they want."[65]

89. USDS/DOGE representatives have also been caught installing "hard drives" and a "new server being used to control" EHRI and other databases at OPM.[66]

90. In addition to EHRI, USDS/DOGE also has access to other OPM systems.[67] These systems include: USAJOBS, the federal government's hiring site that contains the personal information, including Social Security Numbers, home addresses, and employment records, of anyone who has applied for a federal job or internship; USA Staffing, an onboarding system; USA Performance, a job performance review site; and HI, a system for managing employee health care that contains sensitive health information protected by the Health Insurance Portability and Accountability Act ("HIPAA").[68]

91. The identities of the USDS/DOGE personnel who have access to Treasury and OPM systems and to whom sensitive information has been disclosed are not yet clear, and to the extent there is available information on those individuals, it is only available from public reporting. On information and belief, these individuals lack training in applicable security safeguards for personal information, do not have relevant Treasury or OPM experience, may not have necessary security clearances, and may not be federal employees.

---

[65] *Id.*
[66] Alt National Park Service (@altnps.bsky.social), Bluesky (Jan. 31, 2025, 8:14 PM ET), https://bsky.app/profile/altnps.bsky.social/post/3lh3dl3rkgc2u.
[67] *Id.*
[68] *Id.*

92. Wired has identified six members of the USDS/DOGE as men between the ages of 19 and 24 with "little to no government experience."[69]

93. According to public reporting, Akash Bobba, Ethan Shaotran, Edward Coristine, and Luke Farritor all have working GSA email addresses and access to all GSA systems. Bobba and Coristine are both also listed as OPM "experts." Gavin Kliger is listed as "special advisor to the director for information technology in internal records and as "special advisor to the OPM director" on his LinkedIn.

94. Gautier Cole Killian has a working DOGE email address and is listed as a "volunteer."

95. By granting EHRI system access to USDS/DOGE, OPM disclosed vast stores of personal information contained in those systems to individuals not authorized by law to access them; for purposes impermissible under the Privacy Act and the applicable systems of records notice and privacy impact assessments; and in violation of established security policies and requirements.

Harms to Plaintiffs

96. Plaintiffs have a constitutional right to the privacy of their information; Treasury and OPM Defendants have violated and continue to violate that right by unlawfully disclosing extremely personal information about Plaintiffs and millions of others to unchecked actors in violation of law.

[69] Vittoria Elliott, *The Young, Inexperienced Engineers Aiding Elon Musk's Government Takeover*, WIRED (Feb. 2, 2025), https://www.wired.com/story/elon-musk-government-young-engineers/.

97. The ongoing breach of Treasury and OPM systems puts Plaintiffs at severe continuous risk of further data disclosure.

98. Elon Musk has disclosed sensitive information from Treasury systems over a publicly accessible social media platform, including, but not limited to, his 215 million "followers." On information and belief, he received access to that information through and because of his affiliation with DOGE Defendants.

99. DOGE Defendants and other DOGE operatives have made clear their disregard for legal controls or restraints, and in light of their past willingness to disclose information publicly or use it for other unlawful purposes, their continued access to sensitive information presents a near certainty that they will continue to misuse that information.

100. The use of unauthorized and unsecured information technology to access, view, store, or disseminate sensitive information creates increased vulnerability to illegal exfiltration by actors unaffiliated with the federal government or DOGE.

101. Specifically, OPM and Treasury data are rich targets for cyberattacks both by criminals and by foreign adversaries.

102. The PII contained in both systems can enable identity theft and other financial crimes which have devastating effects on their victims. Plaintiffs' information is at significantly elevated risk of being stolen and used by cybercriminals for these purposes.

103. OPM data have already likely been targeted in prior breaches by foreign adversary actors to gain intelligence or other advantage over the United States, specifically to the detriment of the individuals whose information was stolen.

104. Foreign adversaries regularly target United States government information systems, and increasing the vulnerability of desirable data creates an elevated risk that they will successfully access those data.

Count I
Violation of the APA: Unlawful Agency Action (FISMA)
Government Defendants

105. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

106. Treasury Defendants and OPM Defendants have administered systems containing vast quantities of sensitive personal information without complying with statutorily required security protections under FISMA. 44 U.S.C. §§ 3554(a)(1)–(2).

107. Defendants Treasury Department and OPM have thereby engaged in conduct that is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(A).

108. Defendants' conduct constitutes final agency action under 5 U.S.C. § 704.

109. Treasury Defendants and OPM Defendants' failure to maintain and comply with required security protections resulted in unlawful access to OPM and Treasury systems, violating Plaintiffs' constitutional right against disclosure of personal matters, harming their privacy interests, and exposing their private information to heightened risk.

Count II
Violation of the Privacy Act
Government Defendants

110. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

111. Treasury Defendants and OPM Defendants have disclosed Plaintiffs' personal data contained in systems of records controlled by Defendants in violation of the Privacy Act, 5

U.S.C. § 552a(b) and wrongfully used such data for computer matching without an adequate written agreement in violation of the Privacy Act, 5 U.S.C. § 552a(o).

112. Plaintiffs are entitled to civil remedies under 5 U.S.C. § 552a(g).

Count III
Violation of 26 U.S.C. § 6103
(Willful or Grossly Negligent Unauthorized Disclosure)
Defendants Scott Bessent, U.S. Treasury

113. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

114. The Treasury Department maintains records of direct payments and direct deposits for tax payments and refunds for up to six years from the date of the direct deposit. IRM 12.4.2.1.2.1.2.

115. Plaintiff Doe 1's return information has been used by BFS systems to process tax payments in the last 6 years. Information about those transactions is included in BFS systems.

116. Treasury, Secretary Bessent, and DOGE have knowingly or grossly negligently violated Section 6103 by disclosing and inspecting confidential return information contained in the BFS system, which includes tax return information (including the amount of tax refunds), including Doe 1's.

117. Pursuant to 26 U.S.C. § 7431, Plaintiff Doe 1 is entitled to statutory damages in the amount of $1,000 per each act of unauthorized inspection and disclosure.

118. Plaintiff Doe 1 is also entitled to punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because the Treasury Department and DOGE's unlawful disclosure of their confidential return information was either willful or a result of gross negligence.

Count IV
Violation of the Fifth Amendment (Right to Informational Privacy)
Government Defendants

119. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

120. Defendants, by providing access to confidential personal information, including financial information, in which individuals have a reasonable expectation of privacy, without lawful authorization, have deprived EPIC's members and Doe 1 of their liberty interest in avoiding disclosure of personal matters under the Due Process Clause of the Fifth Amendment. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Payne v. Taslimi*, 998 F.3d 648, 656 (4th Cir. 2021).

121. Defendants have done so without legal authorization, without providing notice to the individuals whose data has been accessed, including EPIC's members and Doe 1, and without providing them an opportunity to challenge the disclosure of their data before a neutral decisionmaker.

122. Defendants have violated the Fifth Amendment rights to due process of law of Plaintiff EPIC's members and of Plaintiff Doe 1. U.S. Const. amend. V.

Count V
Actions *Ultra Vires*/Mandamus
DOGE Defendants

123. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

124. In directing and controlling the use and administration of Defendant OPM's EHRI system and Defendant Treasury Department's BFS payment systems, DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of people.

125. DOGE Defendants may not take actions which are not authorized by law.

126. No law or other authority authorizes or permits DOGE defendants to access or administer these systems.

127. Through such conduct, Defendants have engaged (and continue to engage) in *ultra vires* actions which injure plaintiffs by violating their constitutional rights, exposing their private information, and increasing the risk of further disclosure of their information.

128. Plaintiffs are entitled to a writ of mandamus directing the Acting USDS Administrator to remedy these violations.

Requested Relief

WHEREFORE, Plaintiffs request that this Court:

1. Enjoin Defendants' wrongful provision of access and disclosure personal information in the OPM system (Enterprise Human Resources Integration) and Treasury systems (Bureau of Fiscal Services);
2. Declare unlawful and halt Defendants' use of OPM and Treasury systems for purposes in excess of System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and the Federal Information Security Modernization Act (FISMA);
3. Declare unlawful and halt OPM Defendants and Treasury Defendants from sharing data from OPM systems and Treasury systems with non-agency employees for non-routine and non-permitted purposes;
4. Declare unlawful and halt DOGE Defendants' direction or control of use of OPM and BFS systems;
5. Declare unlawful and halt DOGE Defendants' access to or disclosure of personal or other protected information;

6. Order Defendants to disgorge or delete all unlawfully obtained, disclosed, or accessed personally identifiable information from systems or devices on which they were not present on January 19, 2025;
7. Order Treasury Defendants and OPM Defendants to establish and maintain security protections that prevent the unauthorized access of such information;
8. Order Treasury Defendants and OPM Defendants to revoke access to personal information by DOGE Defendants and any other unauthorized entity or individual;
9. Prohibit DOGE Defendants from collecting, accessing, disclosing, or retaining personal information in OPM systems and Treasury systems;
10. Award statutory and punitive damages to Plaintiff Doe;
11. Award costs and reasonable attorneys' fees incurred in this action; and
12. Grant such other relief as the Court may deem just and proper.

Dated: February 10, 2025

Respectfully Submitted,

/s/ Matthew B. Kaplan
Matthew B. Kaplan, VSB # 51027
THE KAPLAN LAW FIRM
1100 N. Glebe Rd., Suite 1010
Arlington, VA 22201
Telephone: (703) 665-9529
mbkaplan@thekaplanlawfirm.com

Alan Butler*
EPIC Executive Director
John L. Davisson*
EPIC Director of Litigation
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (fax)

Mark B. Samburg*
Aman T. George*
Orlando Economos*
Robin F. Thurston*
Skye Perryman*
DEMOCRACY FORWARD FOUNDATION
P.O. Box 34553
Washington, D.C. 20043
Telephone: (202) 448-9090
Fax: (202) 796-4426
msamburg@ democracyforward.org
ageorge@democracyforward.org
oeconomos@democracyforward.org
rthurston@democracyforward.org
sperryman@democracyforward.org

*pro hac vice *application forthcoming*

Counsel for Plaintiffs