UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CENTER FOR TAXPAYER RIGHTS,
P.O. Box 71278 Washington DC 20024

MAIN STREET ALLIANCE,
909 Rose Ave, Suite 400
North Bethesda, MD 20852

NATIONAL FEDERATION OF FEDERAL EMPLOYEES, IAM AFL-CIO
1225 New York Avenue, NW
Suite 450
Washington, DC 20005

COMMUNICATIONS WORKERS OF AMERICA, AFL-CIO
501 3rd Street, NW
Washington, DC 20001,

Plaintiffs,

vs.

INTERNAL REVENUE SERVICE
1111 Constitution Ave., NW,
Washington, DC 20224

DOUGLAS O'DONNELL, in his official capacity as Acting Commissioner, Internal Revenue Service,
1111 Constitution Ave., NW,
Washington, DC 20224

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

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

U.S. DIGITAL SERVICE (U.S. DOGE

Case No. 25-cv-
Jury Trial Requested

SERVICE)
736 Jackson Pl NW
Washington, DC 20503

U.S. DOGE SERVICE TEMPORARY ORGANIZATION
736 Jackson Pl NW
Washington, DC 20503

Defendants.

PLAINTIFFS' COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. Since President Trump's inauguration on January 20, the "U.S. DOGE Service," apparently led by White House official Elon Musk, has launched a sweeping campaign to access highly-sensitive information systems and dismantle and restructure multiple federal agencies unilaterally.

2. The speed of these efforts is core to the project. At every step, DOGE is violating multiple laws, from constitutional limits on executive power, to laws protecting civil servants from arbitrary threats and adverse action to crucial protections for data held by the government collected on hundreds of millions of Americans.

3. The results have already been catastrophic. DOGE has seized control of some of the most carefully protected information systems housed at the Treasury Department, the Department of Labor, the Department of Health and Human Services, and the Consumer Financial Protection Bureau, and taken hold of all sensitive personnel information at the Office of Personnel Management.

4. DOGE's spread through the government continues to be rapid, now reaching the Internal Revenue Service ("IRS"). This case seeks to protect the privacy and the legal rights of millions of Americans, and thousands of small business owners, who depend upon the IRS.

5. While the DOGE playbook at the IRS appears to mirror every other agency it has entered, the systems at issue, and the laws that govern access to them, are not.

6. This nation already once experienced a President who sought to collect tax information on his political allies and enemies in the White House for use for favor and punishment and, following the Watergate era, Congress clearly and unequivocally acted to protect the American people from these intrusions.

7. The IRS houses some of the nation's most sensitive information systems. Recognizing the sensitivity of confidential taxpayer information, Congress has enacted specific protections governing access to the information well beyond those that apply to other personal information held by the government.

8. Despite these significant protections, DOGE employees continue to seek unfettered and unlawful access to the information.

9. DOGE claims power and authority that Congress has never granted it, and that it may not legally exercise.

10. As detailed below, DOGE's access to sensitive information systems lacks statutory authority and violates the Tax Reform Act, the Privacy Act, and the Administrative Procedure Act.

11. Absent this Court's intervention, DOGE will have access to highly sensitive data, including social security numbers, information about individuals' income and net worth; bank

account information; tax liability; sensitive information regarding deductions, such as charitable donations and dependents; and whether an individual's tax return has or is being investigated.

12. DOGE will also have access to confidential business information, including profit and loss statements, payroll information, and other sensitive business information.

13. DOGE will have access to information about IRS investigations and reports on suspected tax fraud activity, which could include investigations or reports pertaining to Mr. Musk's businesses or those of his competitors.

14. DOGE will also have access to tax records of Mr. Musk's business competitors, which are held by the IRS. No other business owner on the planet has access to this kind of information on his competitors, and for good reason.

15. Plaintiffs file this complaint and seek a temporary restraining order to maintain the status quo until the Court has an opportunity to more fully consider the illegality of the Defendants' actions.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under federal law, specifically the Tax Reform Act, 26 U.S.C. §§ 6103, 7213A, the Privacy Act, 5 U.S.C. § 552a, and the Administrative Procedure Act, 5 U.S.C. § 701, *et seq*.

17. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) because Defendants are (or purport to exercise the authority of) agencies of the United States and officers or employees of those federal agencies who are sued in their official capacity. Further, Defendants are headquartered in the District of Columbia, where a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred.

PARTIES

18. Defendant the Internal Revenue Service ("IRS") is a federal agency headquartered in Washington, D.C. established to help America's taxpayers understand and meet their tax responsibilities and to enforce the Internal Revenue Code and other tax laws.

19. Defendant Douglas O'Donnell is the Acting Commissioner for the IRS and is sued in his official capacity.

20. Defendant U.S. Department of the Treasury ("Treasury") is a federal Department headquartered in Washington, D.C., and the IRS is a component bureau of Treasury.

21. Defendant Scott Bessent is the Secretary of the Treasury and is sued in his official capacity. Together, IRS, Treasury, Acting Commissioner O'Donnell, and Secretary Bessent will be referred to as the "IRS Defendants."

22. Defendant U.S. DOGE Service (previously the U.S. Digital Service) was established by Executive Order 14158, reorganizing and renaming the United States Digital Service as the United States DOGE Service, established in the Executive Office of the President. Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025).

23. Defendant U.S. DOGE Service Temporary Organization is a temporary organization also created by Executive Order 14158 and headed by the U.S. DOGE Service Administrator. *Id.* Together Defendant U.S. DOGE Service and U.S. DOGE Service Temporary Organization will be referred to as "DOGE" or the "DOGE Defendants." Upon information and belief, Elon Musk, a special government employee, is the acting Administrator for USDS or is otherwise directing the work of the U.S. DOGE Service and the leader of the DOGE Defendants.

24. All Defendants together will be referred to as "the Government Defendants."

25. Plaintiff Center for Taxpayer Rights (the "Center" or "CTR") is a 501(c)(3) not-for-profit organization, incorporated under the laws of Virginia and headquartered in

Washington, DC, that focuses its work on advancing taxpayer rights, promoting trust in systems of taxation, and increasing access to justice in the tax system, particularly for the most vulnerable populations.

26. In addition, the Center runs a federally-funded Low Income Taxpayer Clinic ("LITC").

27. The Center's LITC provides free representation to low-income taxpayers who have tax disputes with federal, state, or local tax agencies.

28. The close attorney-client relationship between the LITC's legal staff and their low-income clients allow the CTR to advocate for their clients' interests, which would be difficult for them to assert themselves. Many of these clients are involved in disputes with the IRS and fear retribution, while others may not have the resources to protect these privacy interests, or fear reputational harm for being identified as low-income filers that qualify for the ETIC.

29. The LITC's clients include individuals whose taxpayer information is especially sensitive.

30. For example, the LITC represents domestic violence survivors. These individuals are often caught up in the IRS audit and dispute process, because the victims' abusers have often claimed the survivors or their dependents on their tax forms.

31. The LITC also represents a high percentage of Earned Income Tax Credit ("EITC") and Child Tax Credit ("CTC") filers. EITC claimants are audited at a rate approximately four times the rate of the rest of the population and the President's statements suggest they may be a focal point of DOGE's scrutiny.[1]

[1] How do IRS audits affect low-income families?, Tax Policy Center, https://taxpolicycenter.org/briefing-book/how-do-irs-audits-affect-low-income-families (last updated Jan. 2024).

32. The LITC also represents immigrants. Many of these clients want to pay their taxes but are fearful that submitting personal information to the government may lead to harm, despite the protections in place to safeguard the confidentiality of this information.

33. Plaintiff Main Street Alliance ("MSA"), headquartered in Maryland and incorporated in Washington, DC, is a nationwide network of small businesses with members across the country.

34. MSA works to help small businesses navigate challenges, strengthen their operations, and contribute to vibrant local communities.

35. MSA has small business members who are sole proprietors, partnerships, family-run enterprises, or expanding local companies, with a resultant need to file various forms of individual and business tax returns.

36. MSA's small business members, especially when launching their sole proprietorship businesses, file individual tax returns with incomes low enough to qualify for and claim the EITC, CTC, and other refundable credits.

37. Plaintiff National Federation of Federal Employees ("NFFE"), IAM, AFL-CIO, is an unincorporated association with its principal place of business in Washington, DC, is a national labor union representing approximately 110,000 professional and non-professional federal government workers across the United States.

38. NFFE's ranks include federal government employees paid at the lower grades of the General Schedule Pay Table and Wage Scale.

39. Some of NFFE's lower-income members have been eligible for, claimed, and will claim the Earned Income Tax Credit. Some of NFFE's members have been eligible for, claimed, and will claim the Child Tax Credit.

40. Plaintiff Communications Workers of America, AFL-CIO ("CWA") is a union of hundreds of thousands of public and private sector workers in communities across the United States, Canada, Puerto Rico, and other U.S. territories. Its members work in telecommunications and IT, the airline industry, manufacturing, federal service contracts, news media, broadcast and cable television, education, health care, public service, and other fields. It is headquartered in Washington, DC.

41. Some CWA members have been eligible for, claimed, and will claim the Earned Income Tax Credit. Some CWA members have been eligible for, claimed, and will claim the Child Tax Credit.

LEGAL FRAMEWORK

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

43. Information systems at the IRS are subject to even more stringent privacy protections given the breadth and sensitivity of the confidential information regarding individual Americans they contain.

44. Following the Watergate scandal and the public disclosure of widespread misuse of citizens' tax information for improper purposes, Congress enacted a comprehensive scheme for the control of tax return information collected by the IRS in the Tax Reform Act of 1976. The comprehensive statutory scheme, codified at 26 U.S.C. § 6103, replaced the prior regime in which return information could be inspected "upon order of the President" and under regulations promulgated by the Secretary of the Treasury and approved by the President.[2]

[2] Mark Berggren, *I.R.C. 6103: Let's Get to the Source of the Problem*, 74 Chi-Kent L. Rev. 825, 825 (1999).

45. Section 6103 requires that tax information, including returns and return information, is to be treated as confidential and subject to inspection or disclosure only when expressly authorized by statute.

46. Even Treasury Department officers and employees are only granted access to inspect or disclose tax information where their "official duties require such inspection or disclosure for tax administration purposes." 26 U.S.C. § 6103(h)(1).

47. 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) (internal citation omitted).

48. In the Taxpayer Browsing Protection Act, Congress made it unlawful even to inspect return information without proper authorization. 26 U.S.C. § 7213A.

49. Taxpayers are also protected explicitly against political interference. Top officials within the Executive Branch, including the President, are prohibited by law from requesting an audit or investigation of a particular taxpayer, or from interfering with an ongoing audit or investigation. 26 U.S.C. § 7217. Violation of this statutory provision is a crime, punishable by fine or imprisonment.

50. For a White House employee to obtain access to return information, the President must personally sign such a request, identifying the specific taxpayer whose return information is

sought and stating "the specific reason why the inspection or disclosure is requested." 26 U.S.C. § 6103(g).

51. 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.

52. 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).

53. The terms "inspected" and "inspection" mean any examination of a return or return information. 26 U.S.C. § 6103(b)(7).

54. 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).

55. The term "return information" encompasses nearly all the information that IRS may possess on individual taxpayers, including

> a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with

> respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense.

26 U.S.C. § 6103(b)(2)(A).

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

57. Other federal laws also protect this information. The Federal Information Security Modernization Act of 2014 ("FISMA"), 44 U.S.C. §§ 3551-59, 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).

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

59. 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).

60. The E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899, requires that agencies conduct a privacy impact assessment for new or substantially changed information technology which contains 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 (updated Feb. 13, 2019).

61. 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 provide 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.

62. Those mandatory standards for Federal information systems can be found in NIST Special Publication 800-53.[3] The standards require that when federal agencies process personally identifiable information ("PII"), they must design and adopt information security and privacy programs to manage the security risks for the PII in the system.[4].

FACTUAL ALLEGATIONS

I. The "Department of Government Efficiency."

63. On November 12, 2024, then President-Elect Trump announced his intent to create the "Department of Government Efficiency" ("DOGE") to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget," to help "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[5] Congress has neither established, nor appropriated

[3] *NIST SP-800-53, Security and Privacy Controls for Information Systems and Organization, Rev. 5*, 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.
[4] *Id*. at 13.
[5] *See* Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, 7:46 PM ET), https://truthsocial.com/@realDonaldTrump/posts/113472884874740859.

money for, DOGE. It appears to be operating at the direction of the President and his White House advisor, Elon Musk.

64. 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 Service as the United States DOGE Service, established in the Executive Office of the President.[6]

65. 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.[7]

66. 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."[8]

67. 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."[9]

68. The E.O. directs Agency Heads to take all necessary steps "to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems,"[10]

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

but makes no mention of this directive being subject to applicable law. The E.O. nominally directs the U.S. DOGE Service to adhere to "rigorous data protection standards."[11]

69. The E.O. does not vest any statutory authority in DOGE.

70. Multiple DOGE officials have asserted that DOGE was reorganized to "fall[] under the Executive Office of the President [EOP]" and is now "subject to [the] Presidential Records [Act],"[12] which applies to, in relevant part, individuals and components in EOP who are close to the President: "a unit or individual of the Executive Office of the President whose function is to advise or assist the President, in the course of conducting activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President." 44 U.S.C. § 2201.

II. DOGE'S Pattern of Rapidly Entering Agencies, Seizing Critical Systems, and Unilaterally Dismantling and Restructuring Them

71. Since Inauguration Day, DOGE personnel have sought and obtained unprecedented access to information systems across numerous federal agencies, including the United States Agency for International Development, the Department of Treasury, the Department of Labor, the Department of Health and Human Services, the Consumer Financial Protection Bureau, the National Oceanic and Atmospheric Administration, the Office of Personnel Management, and the Department of Education.

[11] *Id.*

[12] Minho Kim, *Trump's Declaration Allows Musk's Efficiency Team to Skirt Open Records Laws*, N.Y. Times (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/us/politics/trump-musk-doge-foia-public-records.html?smid=url-share; *see also* Katie Miller (@katierosemiller), X (Feb. 5, 2025, 5:26 PM), https://x.com/katierosemiller/status/1887311943062499425 (contending that the E.O. made DOGE "subject to Presidential Records [Act]").

72. DOGE personnel also played critical roles in the dismantling of the U.S. Agency for International Development and ongoing concurrent efforts to largely cripple the Department of Education.

73. Specifically at the Department of Education, reports indicate that DOGE staff may have already accessed systems that contain protected return information that the Department of Education obtains from the IRS under 26 U.S.C. § 6103 (l)(13) on a controlled basis for the purpose of administering federal student aid.[13]

74. DOGE's behavior repeats itself across virtually every agency it enters: swooping in with new DOGE staff, demanding access to sensitive systems, taking employment action against employees who resist their unlawful commands, and then beginning to re-work the agencies at their will. This process moves incredibly quickly, with agencies transformed roughly overnight, or fully dismantled within a week.

75. Many DOGE staffers appear to be working across multiple agencies concurrently,[14] potentially collecting sensitive information from multiple databases across

[13] *See* Laura Meckler et al., *Trump Preps Order to Dismantle Education Dept. as DOGE Probes Data*, Wash. Post (Feb. 3, 2024), https://www.washingtonpost.com/education/2025/02/03/trump-education-department-dismantling-executive-order-draft/ ("At least some DOGE staffers have gained access to multiple sensitive internal systems, the people said, including a financial aid dataset that contains the personal information for millions of students enrolled in the federal student aid program.").

[14] *See*, *e.g.*, Tim Marchman & Matt Giles, *This DOGE Engineer Has Access to the National Oceanic and Atmospheric Administration*, Wired (Feb. 5, 2025), https://www.wired.com/story/doge-engineer-noaa-data-google-musk-climate-project-2025/; Vittoria Elliott et al., *The US Treasury Claimed DOGE Technologist Didn't Have 'Write Access' When He Actually Did*, Wired (Feb. 6, 2026), https://www.wired.com/story/treasury-department-doge-marko-elez-access/; Avi Asher-Schapiro et al., *Elon Musk's Demolition Crew*, ProPublica (Feb. 6, 2025), https://projects.propublica.org/elon-musk-doge-tracker/ (DOGE staffer Nikhil Rajpal working at NOAA, CFPB, and OPM); Ella Nilsen & Sean Lyngaas, *Trump Energy Secretary Allowed 23-Year-Old Doge Rep To Access It Systems Over Objections From General Counsel*, CNN (Feb. 7, 2025), https://www.cnn.com/2025/02/06/climate/doge-energy-department-trump/index.html (DOGE staffer Luke Farritor working at HHS and Department of Energy); Evan Weinberger, *Musk's DOGE Descends on CFPB With Eyes on Shutting It Down*,

agencies and providing opportunities to combine and cross-reference data in ways that were never contemplated by the security plans for those systems.

76. DOGE is reportedly working on building a "chatbot and other AI tools to analyze huge swaths of contract and procurement data" within the General Services Administration, and DOGE has "moved swiftly in recent weeks to bring aboard more AI tools" into the federal government.[15]

77. DOGE is also reportedly planning to monitor electronic employee communications, including emails, at the agencies it engaged with including monitoring chats and each key stroke typed by employees.[16] And DOGE has, at another agency, reportedly installed software–PuTTY–used for large scale transfers of data.[17]

78. DOGE's careless and unlawful behavior has not ended in merely accessing sensitive and protected information. On February 12, 2025, DOGE posted classified information,

Bloomberg Law (Feb. 7, 2025), https://news.bloomberglaw.com/banking-law/musks-doge-descends-on-consumer-financial-protection-bureau; Asher-Schapiro et al., *supra* (DOGE staffer Gavin Kliger working at CFPB, OPM, and USAID); Makena Kelly & Zoe Schiffer, *Elon Musk's Friends Have Infiltrated Another Government Agency*, Wired (Jan. 31, 2025), https://www.wired.com/story/elon-musk-lackeys-general-services-administration/; Laura Barrón-López (@lbarronlopez), X (Feb. 3, 2025, 2:05 PM), https://x.com/lbarronlopez/status/1886491276729544809 (DOGE staffer Edward Coristine working at OPM, Small Business Administration, and General Services Administration).

[15] Paresh Dave et al., *Elon Musk's DOGE is Working on a Custom Chatbot Called GSAi*, Wired (Feb. 6, 2025), https://www.wired.com/story/doge-chatbot-ai-first-agenda/.

[16] Jenna McLaughlin & Shannon Bond, *GSA Staff Facing Massive Cuts and Fears Of 'nonstop' Surveillance*, NPR (Feb. 12, 2025), https://www.npr.org/2025/02/11/nx-s1-5293258/trump-gsa-budget-cuts-doge ("Some employees were told that this would include monitoring of when employees logged in and out of their devices, when employees swipe in and out of their workspaces and monitoring of all their work chats. They were also told that 'keylogger' software that would keep track of everything the employees typed on their work machines would be installed on their work computers, the GSA officials said.")

[17] David Ingram, *DOGE Software Approval Alarms Labor Department Employees*, NBC News (Feb. 13, 2025), https://www.nbcnews.com/tech/security/doge-software-approval-alarms-labor-department-employees-data-security-rcna191583.

including classified personnel information, from the National Reconnaissance Office on its website.[18]

DOGE's sensitive data takeovers at Treasury and OPM

79. Shortly before President Trump's inauguration, DOGE operatives demanded access to sensitive Treasury systems, including the system used by the Bureau of the Fiscal Service ("BFS"), to control the vast majority of federal payments.[19]

80. The career official serving as Acting Secretary of the Treasury prior to Secretary Bessent's confirmation denied DOGE operatives' request for access to the BFS payment system, and was subsequently placed on administrative leave.[20]

81. Following his confirmation, Secretary Bessent granted DOGE operatives access to BFS, though the precise identities of DOGE personnel with access, and their level of access, are not reliably known by the public.[21]

[18] Jennifer Bendery, *Elon Musk's DOGE Posts Classified Data On Its New Website*, HuffPost (Feb 14, 2025), https://www.huffpost.com/entry/elon-musk-doge-posts-classified-data_n_67ae646de4b0513a8d767112; Will Steakin et al., *DOGE Data Release Criticized By Intel Community; Trump Admin Says It's Public Data*, ABC News (Feb. 16, 2025), https://abcnews.go.com/US/agency-data-shared-doge-online-sparks-concern-intelligence/story?id=118858837.

[19] Katelyn Polantz et al., *How an Arcane Treasury Department Office Became 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.htm.

[20] Jeff Stein et al., *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/.

[21] 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.

82. According to some reporting, DOGE personnel had the ability to stop individual payments from the BFS system, to change data in the system, or to alter system code.[22]

83. On February 8, a judge in the Southern District of New York issued a Temporary Restraining Order halting DOGE's access to Treasury systems, finding that granting DOGE access to those systems "presents the risk of disclosure and confidential information and [a] heightened risk that the systems in question will be more vulnerable than before to hacking." *Order Granting Temporary Restraining Order*, *New York v. Trump*, No. 25 Civ. 1144, slip op. at 2 (S.D.N.Y. Feb. 8, 2025).

84. In the wake of that decision, a decision which Mr. Musk suggested in posts on his social media website X was issued by a "corrupt" judge who "needs to be impeached" and should be ignored,[23] Mr. Musk for the first time described at least some of DOGE's work at Treasury as seeking to ensure that payment categorization codes in outgoing government payments are no longer left blank, requiring every payment to "include a rationale for the payment," and require more frequent updating of Treasury's "DO-NOT-PAY" list.[24] According to Mr. Musk, career Treasury employees rather than DOGE staff will be implementing these changes.[25]

[22] Vittoria Elliott et al., *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/.

[23] Alexandra Marquez, *Legal Experts Warn of 'Constitutional Crisis' as JD Vance and Elon Musk Question Judges' Authority Over Trump*, NBC News (Feb. 9, 2025), https://www.nbcnews.com/politics/white-house/legal-experts-constitutional-crisis-vance-musk-judicial-rulings-trump-rcna191387.

[24] Elon Musk (@elonmusk), X (Feb. 8, 2025, 2:51 PM ET), https://x.com/elonmusk/status/1888314848477376744.

[25] *Id.*

85. Mr. Musk said the DOGE team and Treasury had jointly agreed to this work, although he did not indicate whether it was the full extent of DOGE's work and plans in Treasury's sensitive systems.[26]

86. DOGE personnel followed a similar pattern to seize control of OPM systems, which contain significant personally identifiable information about federal job applicants, employees, and retirees, including information about employees in the Judicial Branch and the Congressional Branch. On January 20, 2025, DOGE affiliates moved into OPM headquarters, eventually setting up sofa beds on the building's fifth floor, which contains the OPM Director's Office.[27]

87. DOGE personnel directed OPM staff to grant them high-level access to OPM computer systems, and quickly took control of them, including systems containing large troves of personally identifiable information. DOGE personnel also locked career civil servants at OPM out of at least some of those systems, giving them completely unchecked control over the systems and the information they contain.[28]

88. The identities of the 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.

III. DOGE Seeks Access to Protected Information at IRS

89. DOGE and its game of governmental whack-a-mole has wreaked havoc on the American system of government (perhaps a feature not a bug of its aims) and caused incredible

---

[26] *See id.*

[27] *Id.*

[28] Tim Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, Reuters (Feb. 2, 2025), https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.

concern for the privacy of the American public. It has not helped that the federal government has been unable to articulate exactly what DOGE is, its activities, or the authorities under which it is operating; nor has it been able to articulate exactly how DOGE employees are simultaneously members of multiple agencies at the same time–even as they assert that DOGE is now no longer a part of OMB and is subject to the Presidential Records Act, implying that DOGE is a component close to the President within the White House.[29]

90. Whatever clear lines DOGE may seek to blur with regard to other agencies and data sets, its arrival at the IRS and attempt to obtain sensitive tax information puts things precisely in focus.

91. The nation has, once before, experienced an executive branch that sought to obtain information regarding individual American taxpayers and Congress put an unambiguous barrier in its way. Those protections, enshrined in federal law for decades, mandate that DOGE be restrained here.

Historical Abuses Prompted Stringent Protection of Return Information

92. In the 1970s, the Watergate hearings revealed that the Nixon White House had sought to access IRS return information concerning both supporters under audit and individuals on its "enemies" list. The Nixon Administration had also authorized broad access to inspect all farmers' return information for "statistical purposes."[30]

[29] Minho Kim, *Trump's Declaration Allows Musk's Efficiency Team to Skirt Open Records Laws*, N.Y. Times (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/us/politics/trump-musk-doge-foia-public-records.html?smid=url-share; *see also* Katie Miller (@katierosemiller), X (Feb. 5, 2025, 5:26 PM), https://x.com/katierosemiller/status/1887311943062499425 (contending that the E.O. made DOGE "subject to Presidential Records [Act]").

[30] Nat'l Taxpayer Advocate, *Annual Report to Congress* 241 (2003), https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2020/08/nta_2003_annual_update_mcw_1-15-042.pdf.

93. Following these abuses, the Tax Reform Act of 1976 added new protections and a stringent regime of confidentiality to return information in the IRS's control.

94. The importance of these protections remains clear today, as President Trump's former chief of staff has stated that the president expressed a desire in his first term to have the IRS investigate or audit his perceived political enemies.[31]

At IRS, Access to Return Information Is Tightly Controlled Even to IRS Employees Due to Its Extraordinary Sensitivity

95. IRS policy contains detailed protocols to protect privacy that apply to ensure even IRS employees only access return information for tax administration purposes.[32]

96. These policies require that IRS employee access to sensitive personal information like return information occur according to standard operating procedures and within the bounds of privacy protection plans.[33]

97. For example, return information must only be placed in shared locations with "strong access controls" based on "need-to-know principles."[34]

98. IRS policy states that "IRS employees may access returns and return information only when there is a 'need to know' the information for their tax administration duties," and that a "need to know" must "be established on a *case by case basis*."[35]

99. IRS employees are "only allowed to access tax return information when it is needed to carry out their assigned tax administrative duties," and IRS employees are directed to

[31] Michael S. Schmidt, *Trump Wanted I.R.S. Investigations of Foes, Top Aide Says*, N.Y. Times (Nov. 13, 2022), https://www.nytimes.com/2022/11/13/us/politics/trump-irs-investigations.html.
[32] Internal Revenue Manual 10.5 (IRS 2020), https://www.irs.gov/irm/part10/irm_10-005-002.
[33] Internal Revenue Manual 10.5.2.1.1, 10.5.2.1.3 (IRS 2020), https://www.irs.gov/irm/part10/irm_10-005-002#idm140196468618800.
[34] Internal Revenue Manual 10.5.2.2.5.2 (IRS 2020), https://www.irs.gov/irm/part10/irm_10-005-002#idm140196468618800.
[35] Internal Revenue Manual 11.3.22.2.1 (IRS 2024), https://www.irs.gov/irm/part11/irm_11-003-022 (emphasis added).

consult with their supervisors or other IRS authorities when there is any uncertainty about whether access to return information is authorized.[36]

100. If an IRS employee even inadvertently, or questionably, accesses return information—in error or because such information was merely *related* to the employee's assigned case—they are directed to complete and sign Form 11377 and send it to their manager, documenting their inadvertent access to return information that was not required for their duties.[37]

101. IRS regularly investigates cases of unauthorized access of return information by its own employees, has implemented technological controls to prevent unauthorized access, tracks the access of its personnel, and requires extensive training to protect return information.[38]

102. The Treasury Inspector General for Tax Administration is the component charged with conducting audits and investigations of IRS operations, including reporting on IRS employee misconduct allegations.[39] In carrying out its responsibilities, the Inspector General for Tax Administration regularly investigates, identifies, and refers for criminal prosecution instances of fraud, and issues reports on systemic fraud and waste.[40]

DOGE Access to Sensitive and Personal Information About Taxpayers, Including Social Security Numbers, Banking Information, and Tax Returns.

---

[36] Internal Revenue Manual 10.5.5.3.5 (IRS 2023), https://www.irs.gov/irm/part10/irm_10-005-005.
[37] *Id.*
[38] U.S. Gov't Accountability Off., *Taxpayer Information Keeps Ending Up In the Wrong Hands. What Can IRS Do To Better Protect It?* (Sept. 26, 2023), https://www.gao.gov/blog/taxpayer-information-keeps-ending-wrong-hands.-what-can-irs-do-better-protect-it.
[39] Pub. L. No. 105-206, 112 Stat. 685 (1998).
[40] *See* Treasury Inspector Gen. for Tax Admin., *Recent Investigative Activities*, https://www.tigta.gov/recent-investigative-activities (last visited Feb. 16, 2025); Press Release, Treasury Inspector Gen. for Tax Admin., *TIGTA Identifies Fraud Scheme, Alerts IRS to Prevent $3.5 Billion in Potentially Improper Pandemic Tax Credits* (Apr. 24, 2024), https://www.tigta.gov/articles/press-releases/tigta-identifies-fraud-scheme-alerts-irs-prevent-35-billion-potentially.

103. On February 13, reports emerged that a DOGE employee, Gavin Kliger, arrived at the IRS to "examine the agency's operations."[41]

104. In the few weeks since the Trump Administration took office, Kliger has identified himself being employed by at least CFPB, OPM, and USAID.[42] On February 3, Gavin Kliger sent an email from a USAID mail address announcing its headquarters was closed for business.[43] On February 6, CFPB staff were told that Kliger would require access to CFPB data and systems, and he was added to the CFPB staff directory on February 7.[44] On February 13, Kliger arrived at the IRS. And as of February 16, Kliger listed his job on LinkedIn as Special Advisor to the Director at OPM.[45]

105. Kliger attended the IRS meetings with a handful—as many as five—different phones.[46]

106. Kliger reportedly "made a series of requests" to IRS employees and inquired as to

[41] Nathan Layne, *Exclusive: Top Elon Musk Aide Arrives at IRS to Scrutinize Operations, Sources Say*, Reuters (Feb. 13, 2025), https://www.reuters.com/world/us/top-musk-staffer-goes-irs-examine-operations-sources-say-2025-02-13/.

[42] Asher-Schapiro, *supra* note 14 (DOGE staffer Gavin Kliger working at CFPB, OPM, and USAID); Kelly & Schiffer, *supra* note 14.

[43] Edward Wong et al, *Top Security Officials at Aid Agency Put on Leave After Denying Access to Musk Team*, N.Y. Times (Feb. 3, 2025), https://www.nytimes.com/2025/02/02/us/politics/usaid-official-leave-musk.html.

[44] J. David, *DOGE is Now Inside the Cosumer Financial Protection Bureau*, Wired (Feb. 7, 2025), https://www.wired.com/story/doge-access-consumer-financial-protection-bureau-data/; Bobby Allen et al., *Musk's team takes control of key systems at Consumer Financial Protection Bureau*, N.P.R. (Feb. 7, 2025), https://www.npr.org/2025/02/07/g-s1-47322/musks-team-takes-control-of-key-systems-at-consumer-financial-protection-bureau.

[45] Julinanne Mcshanne, *DOGE Worker Says He Was Radicalized by Reading Writer Who Later Denied Holocaust*, Mother Jones (Feb. 16, 2025), https://www.motherjones.com/politics/2025/02/doge-elon-musk-ron-unz-holocaust-substack-post-sailer-vdare-trump/.

[46] Hunter Walker, *Inside The 'Bizarre' Meeting Where DOGE Requested 'Extensive System Access' At IRS*, Talking Points Memo (Feb. 14, 2025), https://talkingpointsmemo.com/news/doge-irs-extensive-system-access.

what each business unit in the IRS does.[47] He also met with IT and compliance staff, including Chief Information Office Rajiv Uppal and Chief Technology Officer Kaschit Pandya.[48]

107. DOGE also reportedly requested to review IRS systems used for internal accounting operations, such as payroll and purchasing.[49]

108. On February 16, it was reported that DOGE was also seeking broad access to IRS tax systems and datasets including the Integrated Data Retrieval System ("IDRS"), and "[u]nder pressure from the White House," the IRS was considering granting such access with a Memorandum already drafted to facilitate such access.[50] Another report stated that granting DOGE staffer Mr. Kilger access to return information was "imminent[]."[51] Deputy Chief of Staff Miller's February 17 interview comments offering reasons for DOGE's access to IRS systems further made clear that DOGE access was imminent.

109. On information and belief, as of February 17, IRS has decided to grant DOGE such access to return information.

110. The IDRS enables "instantaneous visual access" to return information across an extraordinarily broad swath of IRS files including the Taxpayer Information File, which

[47] Pamela Brown, *DOGE Visits the IRS, Putting Staffers on Edge*, CNN (Feb. 13, 2025), https://www.cnn.com/2025/02/13/politics/doge-visits-the-irs-putting-staffers-on-edge/index.html.
[48] Erin Slowey, *DOGE Aide Visits IRS to Look for Ways to Automate Operations (1)*, Bloomberg Tax (Feb. 13, 2025), https://news.bloombergtax.com/daily-tax-report/musk-aide-visits-irs-queries-on-automation-compliance-efforts.
[49] *Id.*
[50] Jacob Bogage & Jeff Stein, *Musk's DOGE Seeks Access to Personal Taxpayer Data, Raising Alarm at IRS*, Wash. Post (Feb. 16, 2025), https://www.washingtonpost.com/business/2025/02/16/doge-irs-access-taxpayer-data.
[51] Alayna Treene & David Goldman, *DOGE Seeks Access to Highly Sensitive Taxpayer Data at IRS*, CNN (Feb. 17, 2025), https://www.cnn.com/2025/02/17/politics/doge-irs-taxpayer-data/index.html.

integrates return information from individual and organizational taxpayers.[52]

111. The IDRS includes the personal identification numbers and bank information of taxpayers in the United States – individual, business, and nonprofit.

112. Specifically, the IDRS includes:

a. Information about taxpayer returns subject to examination;

b. Application information about pending adoptions, such that adoptive parents can claim the dependency exemption and child care credit;

c. Details about the authorization taxpayers have provided to representatives for purposes of sending tax refunds;

d. Bank information for any check for tax refunds returned to the IRS;

e. Taxpayer Identification Numbers and Individual Taxpayer Identification Numbers; and

f. Preparer Tax Identification Numbers.

113. A Trump Administration official reportedly stated that DOGE required this wide-ranging access to the IDRS to "eliminate waste, fraud, and abuse."[53]

114. President Trump, Mr. Musk, and their employees have offered varying reasons why such access is necessary.

115. On February 13, President Trump stated that "Elon" Musk—DOGE's apparent leader—was working on "fraud" and cited a purported "162 billion [dollars] in improper payments" related to the "Earned Income Tax Credit," which is administered by the IRS.[54]

---

[52] IRS, *2023 Document 6209 - ADP and IDRS Information*, § 14 (2023), https://www.irs.gov/privacy-disclosure/2023-document-6209-adp-and-idrs-information.
[53] Bogage & Stein, *supra* note 50.
[54] Alexander Rifaat, *Musk's Team Enters IRS; Trump Vows Scrutiny of Improper Payments*, TaxNotes (Feb. 14, 2025), https://www.taxnotes.com/featured-news/musks-team-enters-irs-trump-vows-scrutiny-improper-payments/2025/02/14/7r3s6;

116. Two days later, on February 15, Mr. Musk retweeted a chart and X thread purporting to show the total usage of refundable tax credits—including the earned income tax credit—and wrote "[s]uch a big jump in a short time doesn't make sense."[55]

117. On February 17, White House Deputy Chief of Staff Stephen Miller said that "DOGE will root out supposed fraud by foreigners who filed bogus returns."[56] He stated there was fraud in the child tax credit payment system and there needed to be programmatic reforms.[57] This statement comports with the recent comments from President Trump and Mr. Musk suggesting that DOGE's engagement at the IRS will, in part, be inspecting fraud related to tax credits.

118. In the same interview, Miller also stated that the access is needed to identify "that unfair politicization is taking place, that unfair targeting is taking place."[58]

119. Then later on February 17, Mr. Musk tweeted a screenshot that suggested that the reason DOGE is "trying to snoop" around IRS records is to investigate the returns of Senators, including Senator Adam Schiff.[59]

Dusty (@thatdudedusty), X (Feb. 13, 2025, 8:07 PM), https://x.com/thatdudedusty/status/1890206250098397257.

[55] Elon Musk (@elonmusk), X (Feb. 15, 2025, 9:36 PM), https://x.com/elonmusk/status/1890953327069782337.

[56] Josh Fiallo, Meet the Gen-Z DOGE Minion Set to Access Taxpayers' Secrets, Daily Beast (Feb. 17 2025), https://www.thedailybeast.com/meet-the-gen-z-doge-goon-gavin-kliger-who-is-set-to-access-taxpayers-secrets/.

[57] Aimee Picchi, *Elon Musk's DOGE Presence at the IRS Raises Concerns About Taxpayer Data Security, Refund Delays*, CBS News (Feb. 17, 2025), https://www.cbsnews.com/news/musk-doge-trump-irs-taxpayer-data-idrs-wyden-warren-letter/.

[58] Lauren Irwin, *Stephen Miller: DOGE Will Restore 'Faith and Confidence' in IRS,* Hill (Feb. 17, 2025), https://thehill.com/policy/technology/5149835-stephen-miller-doge-irs/.

[59] Elon Musk (@elonmusk), X (Feb. 17, 2025, 6:09 PM), https://x.com/elonmusk/status/1891625938108002407.

120. It is highly unusual—and perhaps unprecedented in the contemporary era—to grant political appointees access to personal taxpayer data, and particularly to the IDRS.[60] Even IRS commissioners do not typically have access to all taxpayer data systems.[61]

HARMS TO PLAINTIFFS

121. Plaintiff Center for Taxpayer Rights focuses its work on advancing taxpayer rights, promoting trust in systems of taxation, and increasing access to justice in the tax system, particularly for the most vulnerable populations.

122. The Center will be harmed by DOGE employees' unfettered access to taxpayer information and thus their ability to cross-reference such data against data from other agencies. Such access will harm the Center's ability to encourage trust in the taxpayer process. For example, undocumented immigrants have often been fearful of filing taxes. The Center encourages them to do so, relying on the protections that numerous statutes and IRS policies afford to taxpayer information.

123. Public reports of DOGE access to taxpayer information, and the access to such information itself, will result in taxpayer distrust of the confidentiality of the information they submit to the IRS—particularly among vulnerable populations.

124. This will result in the Center needing to dedicate more resources to facilitating trust in the taxpayer system and to reach low-income or other vulnerable taxpayers and away from other mission-crucial activities. Without assurances that such protections will be respected by DOGE and the agency employees that grant them access to taxpayer information, the Center

[60] Lily Batchelder (@lilybatch), X (Feb. 17, 2025, 12:47 PM), https://x.com/lilybatch/status/1891544934265630939.
[61] Bogage & Stein, *supra* note 50.

will be unable to assure vulnerable populations that their information will be appropriately safeguarded.

125. This will impede the Center's core activities of reaching taxpayers and furthering the rights of taxpayers.

126. In addition, the Center runs a Low Income Tax Clinic (LITC). The LITC's clients are low income taxpayers who have tax disputes with federal, state, or local tax agencies.

127. Plaintiff Main Street Alliance ("MSA") works to help its small business owner members navigate challenges and thrive, as they work toward long-term prosperity. This includes helping small businesses navigate challenges with taxes, tariffs, access to capital, and other matters that affect their members' financial health.

128. Supporting small businesses as they seek to succeed financially is a key part of MSA's mission, and its members' interests will be harmed if DOGE has wide-ranging access to its members' sensitive financial information contained in IRS tax return information databases, including the IDRS.

129. Additionally, as MSA represents small businesses and sole proprietorships, it has members with incomes low enough to qualify for the EITC, and these members have and will file for that credit. To the extent DOGE focuses its inspection on EITC recipients, as President Trump and Mr. Musk have suggested they might, MSA's members are even more likely to suffer harm.

130. Plaintiff National Federation of Federal Employees ("NFFE") represents 110,000 professional and non-professional federal workers, some of whom are paid on the lower end of

the General Schedule and Wage Grade pay systems, and its mission is to, among other things, promote its members' "economic welfare."[62]

131. NFFE and its members will be harmed by DOGE's broad access to its members' sensitive financial information contained in its members' tax return information within the IRS. In particular, NFFE represents some lower-income federal workers who qualify for the EITC and CTC, and these members have and will file for those credits. To the extent DOGE focuses its inspection on EITC recipients, as President Trump and Mr. Musk have suggested they might, NFFE's members are even more likely to suffer harm.

132. CWA's members include hundreds of thousands of public and private sector workers.

133. CWA and its members will be harmed by DOGE's broad access to its members' sensitive financial information contained in its members' tax return information within the IRS. In particular, CWA represents some lower-income workers who qualify for the EITC and CTC, and these members have and will file for those credits. To the extent DOGE focuses its inspection on EITC recipients, as President Trump and Mr. Musk have suggested they might, MSA's members are even more likely to suffer harm.

CLAIMS FOR RELIEF

Count I

Violation of the APA: Unlawful, Arbitrary and Capricious Agency Action (26 U.S.C. §§ 6103, 7213A)

All Defendants

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

135. IRS Defendants unlawfully permitted DOGE Defendants to access and inspect return information protected by 26 U.S.C. § 6103 and 26 U.S.C. § 7213A.

[62] Nat'l Fed'n of Fed. Empls., *About Us*, https://nffe.org/about/ (last visited Feb. 17, 2025).

136. IRS Defendants' actions have been arbitrary and capricious, not in accordance with the law, and in excess of statutory authority. 5 U.S.C. § 706(2)(A, C).

137. *First*, IRS Defendants have permitted, contrary to 26 U.S.C. § 6103(g), (h), DOGE staff to obtain broad access to return information for a broad purpose in a manner that does not comply with specific statutory requirements.

138. *Second*, IRS Defendants have permitted DOGE staff broad access to sensitive return information in an arbitrary and capricious manner that does not comport with historical or existing IRS practice or policies or consider the consequences of such access.

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

Count II

Violation of the APA: Unlawful, Arbitrary and Capricious Agency Action (FISMA)

All Defendants

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

141. IRS 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).

142. IRS Defendants 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).

143. Defendants' conduct constitutes final agency action under 5 U.S.C. § 704. IRS Defendants' failure to maintain and comply with required security protections resulted in continuing unlawful access to IRS systems harming plaintiffs' privacy interests, and exposing their private information to heightened risk.

Count III

Violation of the APA: Unlawful, Arbitrary and Capricious Agency Action (Privacy Act)

All Defendants

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

145. IRS Defendants have disclosed 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).

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

147. IRS Defendants 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).

Count IV

Violation of the Privacy Act

All Defendants

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

149. IRS Defendants have disclosed Plaintiffs' personal data contained in systems of records controlled by Defendants without Plaintiffs' consent and without satisfying any of the conditions identified in 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).

150. Accordingly, and alternatively to Count III, Plaintiffs are entitled to civil remedies under 5 U.S.C. § 552a(g).

Count V

Actions *Ultra Vires*

DOGE Defendants

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

152. In directing and controlling the use and administration of Defendant IRS' systems, DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of people.

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

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

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

Requested Relief

WHEREFORE, Plaintiffs request that this Court:

1. Enjoin Defendants' wrongful provision of access, inspection, and disclosure of return information and other personal information in the IRS system to members of DOGE;

2. Declare unlawful and halt DOGE Defendants' access to, inspection, or disclosure of personal or other protected information;

3. Declare unlawful and halt Defendants' use of IRS systems for purposes in excess of System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and the Federal Information Security Modernization Act (FISMA);

4. Declare unlawful and halt DOGE Defendants' direction or control of use of IRS systems;

5. Order Defendants to disgorge or delete all unlawfully obtained, disclosed, or accessed return information and other personally identifiable information from systems or devices on which they were not present on January 19, 2025;

6. Order IRS Defendants to establish and maintain security protections that prevent the unauthorized access of return information or other personal information;

8. Order IRS Defendants to revoke access to return information or other personal information by DOGE Defendants and any other unauthorized entity or individual;

9. Prohibit DOGE Defendants from collecting, accessing, disclosing, or retaining return information or other personal information in IRS systems;

10. Prohibit DOGE Defendants from installing any software on IRS systems and order any software previously installed be removed;

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 17, 2025

Respectfully Submitted,

/s/ Daniel A. McGrath

Daniel A. McGrath (Bar No. 1531723)
Karianne M. Jones*
Madeline H. Gitomer*
Robin F. Thurston (Bar No. 7268942)
Skye L. Perryman*
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
Tel.: (202) 448-9090
dmcgrath@democracyforward.org
mgitomer@democracyforward.org
kjones@democracyforward.org
sperryman@democracyforward.org
rthurston@democracyforward.org

Counsel for Plaintiffs

Yvette M. Piacsek (Bar No. 980302)
General Counsel
National Federation of Federal
Employees, IAM, AFL-CIO
1225 New York Ave. N.W., Suite 450
Washington, D.C. 20005
Tel.: (202) 216-4428
ypiacsek@nffe.org

*Motion for *pro hac vice* admission
forthcoming

Counsel for Plaintiff NFFE