UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

American Federation of Teachers, *et al.*, *Plaintiffs*, vs. SCOTT BESSENT, in his official capacity as Secretary of the Treasury, *et al.*, *Defendants*.	Case No. 8:25-cv-00430 Date: Time: Place: Judge: Hon. Deborah Boardman

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES OF CIVIL PROCEDURE

OTHER AUTHORITIES

INTRODUCTION

Millions of Americans rely on the Department of the Treasury ("Treasury"), the Office of Personnel Management ("OPM"), and the Department of Education ("Education") for essential services and benefits. They receive tax refunds, federal salaries, social security benefits, and veterans pay through the Treasury. They apply for federal employment and receive health benefits through OPM. They petition for—and receive—loans through Education to finance their pursuits of higher education and schooling. It is no exaggeration to say that collectively, these three agencies and departments provide essential services to nearly every American in one form or another.

To facilitate the provision of these services, all three agencies rely on the American people to provide sensitive personally identifiable information ("PII") like social security numbers, physical addresses, dates of birth, financial information, and more—information that the agencies then store on their data systems. That exchange is not without risk to the public. In the wrong hands, that information can be repurposed for identity theft and financial fraud with devastating consequences for the people whose information has been disclosed; it can also be used as a weapon to target perceived critics or other disfavored individuals for adverse treatment.

Recognizing the potential for great harm when personal information is consolidated in the government, Congress enacted the Privacy Act of 1974. The Act was one of the crucial reforms passed in response to the Watergate scandal: It codified the people's right to privacy in the personal data and information they shared with the government, and it imposed strict limits on who in the government could access this information and under what circumstances.

Since the Act's passage, government agencies and departments have zealously safeguarded the sensitive personal information stored in their systems—a commitment to protection that has been upheld from one administration to the next. Employees at these departments have historically rebuffed requests by even the White House for information contained within their data systems and restricted access on a strict need-to-know basis. By upholding their obligations under the Privacy Act, as they have done historically, all three

agencies upheld their end of the social contract: They used the personal information entrusted to them by the American people only for the purposes for which it was collected and to facilitate routine government functions.

In the last few weeks, Defendants[1] have broken that social contract, and violated the Privacy Act, by granting unfettered access to their data systems and the PII contained within those systems to dozens of individuals operating at the direction of well-known entrepreneur Elon Musk. These individuals purportedly belong to the Department of Government Efficiency ("DOGE"). DOGE was created by an executive order and is not a Congressionally-established Department. Defendants have allowed DOGE representatives to help themselves to the PII contained within Defendants' systems, and to do so for DOGE's improper purposes, which range from disrupting the Treasury's functions to functionally dismantling the Department of Education. They have expressed a desire to feed Americans' sensitive information to artificial intelligence ("AI") tools and software, further enhancing the risk that PII will be disclosed outside of the government. And they have done all of this while withholding information from the American public about who they are and what they have done with the information that they have accessed.

Plaintiffs include Americans who collect veterans benefits, applied for student loans, and worked as federal employees and whose PII is stored in Defendants' systems that have been accessed by DOGE representatives. Plaintiffs also include union organizations whose members' PII is likewise stored within these systems. Together, they seek to vindicate their privacy rights under the Privacy Act and to put an end to DOGE representatives' access to their PII—access to which they did not consent. Defendants' unprecedented decision to abandon their duties as guardians and gatekeepers of tens of millions of Americans' sensitive information stored in their

[1] Defendants are Scott Bessent, in his official capacity as Secretary of the Treasury; the U.S. Department of the Treasury; Charles Ezell, in his official capacity as the Acting Director of the Office of Personnel Management; the U.S. Office of Personnel Management; Denise L. Carter, in her official capacity as the Acting Secretary of Education; and the U.S. Department of Education.

systems has forced Plaintiffs to seek a temporary restraining order from this Court enjoining further unauthorized disclosures while the parties litigate this case.

STATEMENT OF FACTS

I. The Privacy Act of 1974

When President Ford signed the Privacy Act of 1974 into law, he made clear its lofty purpose, which was to "protect[] a right precious to every American—the right of individual privacy." Gerald R. Ford, Statement on Signing the Privacy Act of 1974 ¶ 1, The American Presidency Project (Jan. 1, 1975), https://www.presidency.ucsb.edu/documents/statement-signing-the-privacy-act-1974 ("Privacy Act Signing Statement"). Recognizing the "vital need to provide adequate and uniform privacy safeguards for the vast amounts of personal information collected, recorded, and used" by the government, President Ford praised the Privacy Act for taking the "historic" step of "codifying fundamental principles to safeguard personal privacy in the collection and handling of recorded personal information by Federal agencies." *Id.* ¶ 3.

President Ford was not alone in his assessment of the Act's significance. Senator Ervin, when introducing the bill that would eventually become the Privacy Act, likewise stressed the importance of protecting "one of our most fundamental civil liberties—the right to privacy." U.S. Cong. Senate Comm. on Gov't Operations, 94th Cong., Legislative History of the Privacy Act of 1974, at 3 (2d Sess. 1976), https://web.archive.org/web/20220401081501/https://www.justice.gov/opcl/PAOverview_SourceBook ("Privacy Act Legis. Hist."). Referencing Watergate, Senator Ervin emphasized that "there must be limits upon what the Government can know about each of its citizens" because "[w]hen the Government knows all of our secrets, we stand naked before official power. . . . [W]e lose our rights and privileges." *Id.* at 4. To that end, he believed it was imperative that Congress "act before sophisticated new systems of information gathering and retention . . . produce widespread abuses" within the government. *Id.* at 5.

The Privacy Act was Congress's solution to the threat of unchecked government access to sensitive information belonging to the American people. For more than half a century, the Act has "balance[d] . . . the right of the individual to be left alone and the interest of society in open

government, national defense, foreign policy, law enforcement, and a high quality and trustworthy Federal work force." *See* Privacy Act Signing Statement ¶ 3. It has maintained that delicate balance by requiring federal agencies to "collect, maintain, use, or disseminate any record of identifiable personal information in a matter that assures that such action is for a necessary and lawful purpose" and prevents "misuse." *See* Privacy Act Legis. Hist. at 501.

All agencies that possess a system of records subject to the Privacy Act must publish a Statement of Record Notice ("SORN") in the Federal Register that sets forth the name and location of the system, the categories of individuals whose records are maintained in the system, the categories of records maintained in the system, and "each routine use of the records contained in the system, including the categories of users and the purpose of such use," among other information. 5 U.S.C. § 552a(e)(4). Federal agencies are forbidden from disclosing records in their systems absent written request or prior written consent by the person whose records are at issue, except in specifically delineated circumstances. *Id.* § 552a(b). One such circumstance is disclosure to an officer or employee of the agency that maintains the record and who has "a need for the record in the performance of their duties" for the agency. *Id.* § 552a(b)(1). Another such circumstance is when disclosure of the record is "for a routine use"—that is, for a use "compatible with the purpose for which it was collected" and described in a SORN published by the agency that maintains the record. *Id.* § 552a(a)(7), (b)(3).

II. Defendants' Data Systems

As technology has advanced over the decades, the government's various data systems have swelled in size and the protections of the Privacy Act have become increasingly important. Combined, Defendants' data systems hold PII for tens of millions of Americans across the country, including but not limited to social security numbers, incomes, addresses, bank account numbers, and dates of birth, which are used to disburse social security benefits, manage health benefits for federal employees, and facilitate federal student loans. Am. Compl. ¶ 48 nn.22–23, ¶ 73 nn.60–61, ¶ 96 n.86, ¶ 97 n.87. Consistent with the Privacy Act, federal agencies have—until now—zealously guarded access to these systems even within their respective departments.

(i) The Treasury Department's Federal Disbursement System

Treasury oversees and maintains the Federal Disbursement Services ("FDS"), which provides critical payment services for hundreds of federal agencies. *Id.* ¶ 46 n.20. Requests for payment, once authorized by other federal agencies, are routed to the FDS for disbursement. *Id.* ¶ 50 n.27. Neither Treasury nor its subdivision, the Bureau of the Fiscal Service, where the FDS is housed, exercise independent judgment as to whether a payment already approved for disbursement by another agency should be disbursed. *Id.*

Last fiscal year, FDS disbursed more than 1.27 billion payments, valued at more than $5.45 trillion. *Id.* ¶ 47 n.21. More than 70 million Americans—including Plaintiffs—rely on FDS's disbursements for federal income-tax refunds, veterans' pay, and social-security benefits. *Id.* ¶ 46 n.20. To facilitate these disbursements, FDS includes extensive PII for recipients of these funds, including names, Social Security numbers, dates and locations of births, physical addresses, telephone numbers, and financial-institution information, among other PII. *Id.* ¶ 48 n.22; *see, e.g.*, Decl. of Clifford "Buzz" Grambo ¶¶ 6–7 ("Grambo Decl."); Decl. of Sarah Tammelleo ¶¶ 6–7 ("Tammelleo Decl.").

Historically, Treasury has restricted access to the FDS and its trove of PII to a small group of career employees that oversee the FDS's operations. *Id.* ¶ 49 nn.24–26. In 2020, Treasury published a SORN describing each of the systems of records within the FDS. *See* Privacy Act of 1974; System of Records, 85 Fed. Reg. 11776 (Feb. 27, 2020). The SORN additionally lists 19 "routine uses" for which prior written consent of the person whose record is being accessed is not required. *Id.* These include uses that are obviously connected to Treasury's functions, such as performing payment processing services, disclosures to federal, state, and local agencies for tax purposes, disclosures to private creditors for the purpose of garnishing wages of an employee if a debt has been reduced to a judgment, and responding to a breach of Treasury records. *Id.* at 11777–78; *see* Grambo Decl. ¶ 7 ("I provided this personal information [to Treasury] in order to access essential services like disability payments and my military pension."). These routine uses do not include access to FDS's payment systems and the

PII contained within for the purpose of halting already-approved disbursements. Notably, until this year, it was "extremely unusual" for anyone with a connection to political appointees to request, much less gain access to, the FDS's payment systems. Am. Compl. ¶ 49 n.25.

(ii) The Office of Personnel Management's Data Systems

OPM serves as the "chief human resources agency and personnel policy manager for the Federal Government." *Id.* ¶ 71 n.58. As part of its responsibilities, OPM maintains data systems for USAJOBS, the Enterprise Human Resources Integration Data Warehouse ("EHRI DW"), USA Staffing, USA Performance, and the Health Insurance Data Warehouse ("HI DW"), among others. *Id.* ¶ 78 n.67. Together, these systems contain PII for tens of millions of individuals, including current and former federal employees as well as applicants for federal jobs. *Id.* ¶ 73 nn.60–61. These systems include PII and sensitive information such as names, Social Security numbers, employment history, work experience, education, salaries, records of participation in the federal employees' health benefits and insurance programs, addresses, demographic information, and more. *See id.* ¶ 73 n.60; *see, e.g.*, Privacy Act of 1974: Update Existing System of Records, 77 Fed. Reg. 73694, 73694–95 (Dec. 11, 2012) (GOVT-1). All told, OPM houses data for tens of millions of individuals currently or formerly employed at more than 500 federal agencies, including data belonging to Plaintiffs. *Id.* ¶ 73 n.61; *see, e.g.*, Decl. of Donald Martinez ¶ 8 ("Martinez Decl."); Tammelleo Decl. ¶¶ 6–7.

OPM has published SORNs for each of these systems. *See* System of Records Notices (SORN), U.S. Office of Personnel Mgmt., https://www.opm.gov/information-management/privacy-policy/#url=SORNs. Similar to the Treasury Department's FDS payment systems, OPM has historically restricted access to its general personnel records and other system records to "senior career employees" at OPM. *Id.* ¶ 73 n.61. Consistent with this, OPM's SORN for general personnel records states that "[a]ccess to computerized records is limited, through use of user logins and passwords, access codes, and entry logs, to those whose official duties require access." 77 Fed. Reg. 73694, 73,698. OPM's SORNs for its other systems of records contain similar statements on restricting access. *See, e.g.*, Privacy Act of 1974: Update and Amend

System of Records, 79 Fed. Reg. 16834, 16837 (Mar. 26, 2014) (GOVT-5); OPM SORN GOVT-2, U.S. Off. of Personnel Mgmt., https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf. The information contained within OPM is so sensitive that historically, OPM has rebuffed even requests by the White House for certain types of data maintained by OPM. Am. Compl. ¶ 132 n.114.

OPM has also published routine uses associated with each of its SORNs. For example, OPM enumerates many routine uses in connection with its general personnel records system—each of which is closely aligned with the agency's core functions, including but not limited to disclosure to training facilities for training purposes, disclosure to health-insurance carriers to identify enrollment in health-benefit plans, and disclosure to other federal agencies that require relevant information contained within the systems to make hiring decisions. 77 Fed. Reg. 73694, 73696–68. None of the enumerated routine uses for this system or any other OPM system containing information from USAJOBS, EHRI DW, USA Staffing, USA Performance, or HI DW contemplate disclosing records contained within the system for the purpose of mass firing personnel. *See, e.g.*, 79 Fed. Reg. at 16836–87 (GOVT-5), Privacy Act of 1974; System of Records, 89 Fed. Reg. 72902, 72904-05 (CENTRAL-23); *see also* Am. Compl. ¶ 90 n.81.

(iii) The Education Department's Student Loan Systems

Education's responsibilities include managing a series of overlapping federal student-loan systems through its Federal Student Aid office. *See* Federal Student Aid, U.S. Dep't of Educ., https://www.ed.gov/about/ed-offices/fsa. These systems include the National Student Loan Data System ("NSLDS"), the Common Origination and Disbursement System ("CODS"), the FUTURE Act System ("FAS"), and the Financial Management System ("FMS"). Am. Compl. ¶ 95 n.85, ¶ 98 n.88, ¶ 100 n.90, ¶ 102 n.92. The NSLDS is the central database for Title IV student financial aid. *Id.* ¶ 95 n.85. CODS processes information in connection with determining eligibility for federal student aid. *Id.* ¶ 98 n.88. FAS is a database that Education uses to determine eligibility and repayment obligations under the various repayment plans the government offers for federal student loans. *Id.* ¶ 100 n.90. Lastly, FMS primarily interfaces

with all of the aforementioned data systems to centralize all federal student-aid accounting and financial data. *Id.* ¶ 102 n.92.

These student-loan systems collectively contain PII for tens of millions of Americans, including Plaintiffs. *Id.* ¶ 96 n.86; *see, e.g.*, Martinez Decl. ¶ 8; Tammelleo Decl. ¶ 7. In particular, the student-loan systems capture data from applicants and participants—as well as from their parents, spouses, and endorsers—for Title IV programs, such as the Federal Pell Grant Program, the Federal Perkins Loans Program, and the Academic Competitiveness Grant Program. *See* Privacy Act of 1974; System of Records, 88 Fed. Reg. 41942, 41946 (June 28, 2023) (CODS). They also capture data provided by aid applicants of or participants in the Free Application for Federal Student Aid ("FAFSA"), including data on the aid applicant's or aid recipients' spouse or parents. Privacy Act of 1974; System of Records, 88 Fed. Reg. 42220, 42222 (June 29, 2023) (FAS). More than 17.6 million FAFSA forms are completed each year. *See* Olivia Munson, *Looking to Submit This Year's FAFSA? Here Is How the Application Works and Its Eligibility*, USA Today (Apr. 19, 2024), https://www.usatoday.com/story/money/2024/04/19/what-is-fafsa/73382299007. Among the types of PII stored on these systems are social security numbers, names, dates of birth, driver's licenses, demographic data, income and asset information, and addresses. Am. Compl. ¶ 96 n.86, ¶ 97 n.87, ¶ 99 n.89, ¶ 101 n.91, ¶ 102 n.92.

Education has published SORNs for each of these federal student-loan systems, all but one of which state that the "information contained" within these systems is "maintained for various purposes relating to aid applicants and recipients." Privacy Act of 1974; System of Records, 89 Fed. Reg. 44652, 44652 (May 21, 2024) (NSLDS); *see also* 88 Fed. Reg. 41942, 41942 (CODS); 88 Fed. Reg. 42220, 42221 (FAS). The sole exception is FMS, in which "[i]nformation . . . is maintained for the purpose of processing refunds to borrowers or loan holders . . . for overpayments and discharges of Title IV Federal student aid." Privacy Act of 1974; System of Records—Financial Management System (FMS), 73 Fed. Reg. 177, 178 (Jan. 2, 2008).

The SORNs for each of these databases make clear that access is strictly limited. For NSLDS and FAS, which house FAFSA-related data, data access is limited to "authorized NSLDS program personnel and contractors responsible for administering the NSLDS program," 89 Fed. Reg. 44652, 44660, and "Education and contract staff on a 'need-to-know' basis," 89 Fed. Reg. 44652, 42225, respectively. For CODS, which houses data associated with Education's Title IV programs, access is also limited to "Department and contract staff on a 'need-to-know' basis." 88 Fed. Reg. at 41951. Access to FMS is likewise limited to staff on a "need-to-know" basis. 73 Fed. Reg. 177, 179 (FMS).

Education is permitted to disclose information maintained in each of these data systems without individual consent if the disclosure is for a routine use "compatible with the purposes for which the record was collected." 89 Fed. Reg. 44652, 44657 (NSLDS); 88 Fed. Reg. 42220, 42224 (FAS); 88 Fed. Reg. at 41948 (CODS). Such routine uses include disclosures that advance specific program purposes and disclosures that are necessary to respond to any breach of data. 89 Fed. Reg. 41948, 44657 (NSLDS); 88 Fed. Reg. 42220, 42224 (FAS); 88 Fed. Reg. 41948, 41950 (CODS); 73 Fed. Reg. at 177, 178–79 (FMS); *see* Martinez Decl. ¶ 9 ("I provided this personal information in order to access . . . funds to help with educational expenses.").

III. DOGE's Unprecedented Access to Government Data Systems

DOGE representatives' commandeering of some of the most sensitive data systems in the government is unprecedented.

After President Trump won the 2024 presidential election, he announced that Elon Musk would lead an initiative called the "Department of Government Efficiency." *See* Elena Moore, Camila Domonoske & Jeongyoon Han, *Trump Taps Musk to Lead a 'Department of Government Efficiency' with Ramaswamy*, NPR (Nov. 12, 2024), https://www.npr.org/2024/11/12/g-s1-33972/trump-elon-musk-vivek-ramaswamy-doge-government-efficiency-deep-state. Shortly thereafter, Musk's affiliates—many of whom are recent high-school or college graduates—sought access to some of Defendants' data systems and the sensitive PII contained within. Am. Compl. ¶¶ 37 n.10, ¶51 n.28 & 29. In particular, these affiliates repeatedly requested access to

the Treasury's FDS payment systems to shut down disbursements. *Id.* ¶ 51 n.28 & n.29. David A. Lebryk, a senior career civil servant at Treasury, denied their requests. *Id.* ¶ 52 n.31.

Following his inauguration on January 20, President Trump issued an Executive Order replacing the United States Digital Services with DOGE. *Id.* ¶ 33 n.5. On January 24, 2025, representatives of DOGE once again approached Lebryk, who was now Acting Secretary of the Treasury, and demanded that he "immediately shut off all USAID payments using [Treasury's] ultra-sensitive payment processing system." *Id.* ¶ 52 n.30. Lebryk refused, on the basis that stopping payments that other federal agencies have requested and approved was not within the scope of the Treasury's work. *Id.* ¶ 52 n.31. Following Lebryk's refusal, he was placed on administrative leave. *Id.* ¶ 52 n.32. Lebryk eventually chose to retire. *Id.*

In late January, while Lebryk was on administrative leave, Defendants Bessent and the Treasury granted at least two DOGE representatives access to the FDS: Tom Krause, the CEO of Cloud Software Group, and Marko Elez, a 25-year-old DOGE representative and Musk affiliate. *Id.* ¶ 53 n.33 & n.34. Although White House Press Secretary Karoline Leavitt, the Treasury, and representatives of the Treasury initially maintained that Krause and Elez possessed only read-only access to the FDS—which, in any event, would have been sufficient to view and copy the PII stored on FDS—public reporting indicated that their access was not so limited. *Id.* ¶ 56 n.38 & n.39, ¶ 57 n.40. On February 11, 2025, a Treasury official confirmed in a sworn affidavit that Elez did in fact possess both read and write permissions to Treasury's payments systems for a period of time. *See* Decl. of Joseph Gioeli III ¶ 20, New York v. Dep't of Treasury, No. 1:25-cv-1144-JAV (S.D.N.Y. Feb. 11, 2025), ECF. No. 34.

At or around the same time Krause and Elez sought and gained access to the Treasury's FDS payment systems, at least 6 other representatives of DOGE were deployed to OPM and Education to access each entity's respective data systems. Am. Compl. ¶ 76 n.65. Defendants OPM and Acting Director Ezell provided DOGE representatives, including a recent high school graduate, with administrative access to its sensitive systems and databases and revoked access to career officials who have long had access to these systems to fulfill their OPM duties. *Id.* ¶ 77

n.66, ¶ 78 n.67, ¶ 79 n.68. As discussed *supra* p.6, these systems and databases hold PII data from USAJOBS, USA Staffing, USA Performance, the Health Insurance Data Warehouse, and others for federal employees, retired federal employees, and applicants for federal employment.

Neither OPM nor DOGE representatives, including Musk, have articulated any reason why they require sweeping access to OPM's systems, but a White House official was quoted as saying that access was required for "corporate restructuring." *Id.* ¶ 89 n.80. On January 28, 2025, more than 2 million federal employees—including some members of the union Plaintiffs—received an email from OPM, titled "Fork in the Road." *See* Nick Bednar, *Breaking Down OPM's 'Fork in the Road' Email to Federal Workers*, Lawfare (Jan. 30, 2025), https://www.lawfaremedia.org/article/breaking-down-opm-s--fork-in-the-road--email-to-federal-workers; Off. Personnel Mgmt., *Fork in the Road* (Jan. 28, 2025), https://www.opm.gov/fork. The email purportedly offered workers the opportunity to take approximately eight months of paid leave and then resign.

On or before February 3, Defendants Education and Acting Secretary of Education Denise Carter likewise granted approximately 20 representatives of DOGE access to the Department's sensitive data systems. Am. Compl. ¶ 103 n.93. As discussed *supra* pp.7-8, Education's systems include information from tens of millions of Americans who have applied for, or sponsored an application for, student loans or grants managed by Education. After obtaining access, members of DOGE began feeding "sensitive data from across the Education Department into artificial intelligence software." *Id.* ¶ 104 n.96. The software and tools that DOGE is using to review sensitive information is reportedly hosted on cloud-based computers that are located outside of the federal government. *Id.* ¶ 110 n.101. While it is not clear whether DOGE representatives have begun feeding Plaintiffs' PII to these AI systems, neither has that possibility been ruled out. The Washington Post has reported that DOGE and its members plan to replicate the AI process "across many departments and agencies" to sift through information "about spending on employees and programs." *Id.* ¶ 104 n.96. And a declaration filed by the Treasury in a separate action reflects that Elez "automat[ed] the manual review" of sensitive

payment information. Decl. of Vona S. Robinson ¶ 11, New York v. Dep't of Treasury, No. 1:25-cv-1144-JAV (S.D.N.Y. Feb. 11, 2025), ECF. No. 32. Plaintiffs include current and former federal employees and individuals who have applied for and received financial support through Education programs, as well as individuals whose PII information is stored in FDS. *E.g.*, Tammelleo Decl. ¶ 3; Martinez Decl. ¶ 5.

Defendants are aware of the significant security risks posed by DOGE representatives' unfettered access to these systems. An internal threat analysis conducted by the Treasury has designated DOGE as an "insider threat," with its threat intelligence team recommending immediate suspension of DOGE's access. Am. Compl. ¶ 136 n.116. That same threat analysis warned that "[c]ontinued access to any payment systems by DOGE members, even 'read only,' likely poses the single greatest insider risk the Bureau of Fiscal Service"—which oversees FDS within the Treasury—"has ever faced." *Id.* ¶ 136 n.118.

Notwithstanding this warning, Defendants continue to provide DOGE representatives with access to a number of sensitive data systems. One federal court has issued a temporary restraining order blocking DOGE representatives from continued access to the FDS and requiring the destruction of any unauthorized copies of the data contained within FDS, *see* Order, New York v. Dep't of Treasury, No. 1:25-cv-1144-JAV (S.D.N.Y. Feb. 11, 2025), ECF No. 6. Separately, Education has agreed to temporarily prohibit DOGE representatives from accessing its student loan data systems until February 17, 2025. *See* Joint Stipulation, Univ. of Cal. Student Ass'n v. Carter, No. 1:25-cv-00354 (D.D.C. Feb. 11, 2025), ECF No. 12. That agreement does not require Education to retrieve and destroy any copies of PII and confidential information that DOGE representatives have made of the information contained on Education's systems. And, in any event, an undetermined number of DOGE representatives remain at liberty to access OPM's systems without restriction today.

LEGAL STANDARD

A temporary restraining order is a matter of the Court's equitable discretion, and may be awarded upon a showing by the plaintiff "[1] that he is likely to succeed on the merits, [2] that he

is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008); *see ClearOne Advantage, LLC v. Kersen*, 710 F. Supp. 3d 425, 431 (D. Md. 2024) ("The standards for granting a TRO and granting a preliminary injunction are the same.").

ARGUMENT

I. Plaintiffs Are Likely to Succeed on the Merits.

Plaintiffs are likely to succeed on the merits of their suit to enjoin Defendants' unlawful decisions to disclose vast swaths of personally identifiable information to DOGE representatives. Agency disclosures of sensitive, personally identifiable information are carefully circumscribed by the Privacy Act of 1974, which was enacted to "safeguard personal privacy in the collection and handling of recorded personal information by federal agencies." Statement on Signing the Privacy Act of 1974 ¶ 3. Defendants' decisions to disclose plainly violate the Privacy Act's restrictions, and do not fall within any of its exceptions. Those decisions failed to take into account the serious security risks associated with large-scale disclosures of sensitive information to DOGE representatives, many of whom are recent college graduates and at least one of whom has leaked proprietary information before. Defendant Agencies' disclosure decisions are contrary to law, in excess of their statutory authority, and arbitrary and capricious. As a result, they must be enjoined pursuant to the Administrative Procedure Act ("APA").

A. Defendants' Grants of Access to DOGE Representatives Constitute Disclosures of Records Under the Privacy Act

The Privacy Act governs federal agency maintenance of PII, placing strict limitations on an agency's ability to disclose records containing such information. Specifically, it prohibits federal agencies from "disclos[ing] any record which is contained in a system of records . . . to any person, or to another agency" without the authorization of the individual to whom the record pertains. 5 U.S.C. § 552a(b). It is indisputable that Defendants have disclosed records to DOGE representatives within the meaning of the statute.

Courts and agencies alike have defined "disclosure" under the Act "liberally," to include not just a record's dissemination, but also the granting of access to a record. *Wilkerson v. Shinseki*, 606 F.3d 1256, 1268 (10th Cir. 2010) (holding that "disclosure" "include[s] not only the physical disclosure of the records, but also the accessing of private records"); 1795 Privacy Act Guidelines – July 1, 1975, 40 Fed. Reg. 28949, 28953 (July 9, 1975) ("A disclosure [under the Privacy Act] may be either the transfer of a record or the granting of access to a record."). The Act defines a "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency." 5 U.S.C. § 552a(a)(4). In the last few weeks, OPM, Treasury, and Education have granted DOGE officials sweeping access to systems of records that contain millions of records with extensive personally identifiable information about Plaintiffs and their members, including their social security numbers, sensitive financial information, and addresses. Each of these systems has been the subject of a published SORN, *see supra* pp. . Accordingly, Defendants have made "disclosures" of "records" under the Act.

B. The Administrative Procedure Act Authorizes Injunctive Relief to Stop Disclosure Decisions Made in Violation of the Privacy Act

When an agency decides to disclose records in violation of the Privacy Act, the APA authorizes individuals whose information is contained in such records to seek injunctive relief to stop the disclosure. The APA provides that a court must grant review of—and may ultimately enjoin—an agency decision where (1) that decision constitutes a "final agency action"; and (2) there is "no other adequate remedy" available. 5 U.S.C. § 704. Both requirements are met where, as here, a Plaintiff challenges a decision to disclose his or her records in violation of the Privacy Act and there is no other adequate remedy available to prevent Defendants' disclosure. As the Fourth Circuit has expressly recognized, "injunctive relief for a Government's violation of the [Privacy] Act" is "appropriate and authorized by the APA." *Doe v. Chao*, 435 F.3d 492, 505 n.17 (4th Cir. 2006) (citing 5 U.S.C. § 706(2)(A)).

Defendants' decisions to provide representatives of DOGE with access to sensitive record systems constitute "final agency action[s]" subject to judicial review.[2] 5 U.S.C. § 704. The Supreme Court has held that an agency's "decision to disclose" records is a final agency action reviewable under the APA. *Chrysler Corp. v. Brown*, 441 U.S. 281, 318 (1979) (holding an agency's "decision to disclose" reports pursuant to FOIA "is reviewable agency action" under the APA); *see Brancheau v. Sec'y of Lab.*, 2011 WL 4105047, at *2 (M.D. Fla. Sept. 15, 2011) ("In *Brown*, the government agency had already made a decision to release the documents at issue," meaning "there was final agency action."). Here, Defendant Agencies decided to grant DOGE employees unfettered access to systems of records containing PII. As in *Brown*, these "decisions to disclose" are reviewable under the APA.

"[T]here is no other adequate remedy" available to Plaintiffs to redress the harm caused by Defendants' decision to disclose their information. 5 U.S.C. § 704. As the Fourth Circuit recognized in *Chao*, injunctive relief to stop an unlawful disclosure "could not possibly have been obtained, standing alone, under the relevant subsections of the Privacy Act." *Doe*, 435 F.3d at 505. This is because "the Privacy Act makes no provision for injunctive relief to prevent violations of subsection (b) as part of the remedies that it does provide." *Id.* at 504 (cleaned up). Instead, injunctive relief must be obtained via the APA. *Id.* at 505.

C. Defendants' Decisions to Disclose Are Unlawful and Must Be "Set Aside" Pursuant to the Administrative Procedure Act

The APA requires a reviewing court to "hold unlawful and set aside" any agency action that is arbitrary and capricious; "not in accordance with law"; or exceeds the statutory authority of the agency. 5 U.S.C. § 706(2). Defendant Agencies' decisions to disclose must be held unlawful and enjoined on all three grounds.

[2] In determining whether an action constitutes a reviewable "final agency action," this Court applies a "strong presumption that courts may review informal agency adjudication." *Doe v. Tenenbaum*, 127 F. Supp. 3d 426, 459 (D. Md. 2012).

1. Defendants' Decisions to Disclose Are Contrary to Law and Exceed Their Statutory Authority

Defendants' disclosures must be enjoined under the APA because they directly violate the Privacy Act. An agency's decision to disclose records in violation of the Privacy Act "*clearly* is a case of agency action 'not in accordance with law' within the meaning of 5 U.S.C. § 706(2)." *Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988) (emphasis added) (quoting 5 U.S.C. § 706(2)).

Defendants' decisions to disclose violate the Privacy Act because (1) Defendants failed to obtain authorization from the affected individuals prior to disclosure and (2) no statutory exception applies. The records disclosed to DOGE officials include Plaintiff's highly sensitive personal information. *E.g.*, Grambo Decl. ¶ 6. Yet no individual Plaintiff or member of a union Plaintiff consented to these disclosures. *See e.g.*, Martinez Decl. ¶ 10 ("I did not request disclosure of my personal information to DOGE representatives or provide written access authorizing such disclosure."); Tammelleo Decl. ¶ 8 ("not aware of any AFT member who has requested or authorized" DOGE's access). Defendants' decisions to disclose are unlawful under the Privacy Act unless they fall within one of the Act's specifically enumerated exceptions.

None of the Privacy Act's thirteen enumerated exceptions applies. *See* 5 U.S.C. § 552(b). Six of them are for disclosures to consumer reporting agencies and government entities not relevant here. *See id.* § 552(b)(4), (6), (9), (10), (11), (13). Five other exceptions pertain to statistical research, civil or criminal law enforcement activities authorized by law, the health and safety of the individual whose record is the subject of disclosure, court orders authorizing disclosure, and disclosures required by the Privacy Act—all of which are equally inapplicable on their face. *Id.* § 552(b)(2), (5), (7), (8), (12).

The remaining two exceptions authorize disclosure of records (1) "to those officers and employees of the agency . . . who have a need for the record in the performance of their duties", 5 U.S.C. § 552a(b)(1); and (2) pursuant to a "routine use," *id.* § 552a(b)(3). These exceptions do not apply here either.

First, the so-called "need-to-know" provision set forth in § 552a(b)(1) provides a limited exception to the bar on disclosure, permitting disclosure where access to the record is necessary for an agency employee to perform his duties. As an initial matter, this exception applies only to disclosures *within* an agency; it "does not authorize disclosure outside the 'agency.'" *Dick v. Holder*, 67 F. Supp. 3d 167, 177-178 (D.D.C. 2014). It cannot insulate disclosures that were made to DOGE representatives not officially employed by the disclosing agency.

Nor can disclosures made to the DOGE representatives who were named Special Government Employees of the relevant agencies qualify for this exception where disclosures to such employees would undermine the purposes of the Privacy Act. In prior Privacy Act cases, the government has generally invoked the "need-to-know" exception with respect to specific records, and courts carefully scrutinize "whether the official examined the record in connection with the performance of duties assigned to him and whether he *had to do so* in order to perform those duties properly." *Bigelow v. Dep't of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000) (emphasis added); *see Walker v. Gambrell*, 647 F. Supp. 2d 529, 538 n.4 (D. Md. 2009) (reasoning that the "need-to know" exception did not apply where "it is difficult to see how knowledge with such specificity was necessary").

This record-by-record approach is by design. The Privacy Act was enacted in part to ensure that government agencies and their employees accessed only that information necessary to perform their duties and no more. That is the only way Congress could be sure that "we never see the day when a bureaucrat in Washington . . . can use his organization's computer facilities to assemble a complete dossier of all known information about an individual." 120 Cong. Rec. 36,917 (daily ed. Nov. 21, 1974) (statement of Sen. Percy). And the "specific exemptions [to the Privacy Act's bar on disclosure] that Congress established reflect a delicate balance between limiting disclosure of records, and not unduly hampering government operations." *Doe v. DiGenova*, 779 F.2d 74, 84 (D.C. Cir. 1985). In other words, the Privacy Act was designed to avoid *exactly* the sorts of wholesale disclosures authorized by Defendants, which do not "delicate[ly] balance" important competing interests so much as destroy that balance.

Furthermore, proclaiming DOGE representatives to be Special Government Employees does not change the fact that those representatives have been charged with accomplishing goals that are entirely incompatible with the legitimate aims of the Defendant Agencies—namely, firing government employees en mass, Am. Compl. ¶ 91 n.82; cancelling already-approved payments, *id.* ¶ 64 n.47; and "end[ing] the [] Department of Education, *id.* ¶ 116 n.104." None of these are valid agency objectives. *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000) (An agency "may not exercise its authority in a manner that is inconsistent with the administrative structure that Congress enacted into law." (internal quotation and citation omitted)). Allowing Mr. Musk and the agency Defendants to authorize "duties" that are so broad that they could arguably encompass every conceivable piece of government information—and that are contrary to the lawful objectives of the agencies—would gut the Privacy Act. *Cf. Tijerina v. Walters*, 821 F.2d 789, 795 (D.C. Cir. 1987) ("The agency's efforts to elude . . . statutory duties which cannot be shirked under the [Privacy] Act contravene the language of the Act and the purpose behind" the provision at issue.").

Second, Defendants' disclosures to DOGE representatives are not "routine uses." Congress took pains to craft the "routine use" exception in such a way as to "discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." *DiGenova*, 779 F.2d at 84 (quoting 120 Cong. Rec. 40,881 (introduced by Sen. Moorhead)). Accordingly, "for a disclosure to qualify as a 'routine use,' it must be compatible with the purpose for which the agency collected the personal information, and be in accordance with a routine use the agency has published in the Federal Register." *Fattahi v. Bureau of Alcohol, Tobacco & Firearms*, 328 F.3d 176, 178 (4th Cir. 2003) (internal quotations and citations omitted).

Defendants' published SORNs reveal a limited set of routine uses, which are closely tailored to the purposes for which the agencies collected the data. OPM, for instance, has promulgated routine uses that facilitate the agency's core functions as the federal government's personnel hub, including disclosure to training facilities for training purposes, disclosure to

health insurance carriers to identify enrollment in health benefit plans, and disclosure to other agencies that require specific information to make hiring decisions. 77 Fed. Reg. at 73,696-98. Treasury's promulgated routine uses likewise align with its primary directives, such as disclosures to payment processors to facilitate payments and disclosures to other agencies for tax purposes. 85 Fed. Reg. 11,777-78. And Education's promulgated uses include disclosures that hew close to its central mission of advancing specific education programs. 89 Fed. Reg. at 44657 (NSLDS); 89 Fed. Reg. at 42224 (FAS); 88 Fed. Reg. at 41948, 41950 (CODS); 73 Fed. Reg. at 178-79 (FMS).

Defendants, along with Mr. Musk and the President, have publicly trumpeted their rationales for deciding to disclose records to DOGE officials, and none of those rationales fits any of the agencies' promulgated "routine uses," let alone the purposes for which the underlying data was collected. OPM has disclosed records in connection with efforts to facilitate removal of federal employees from their positions en masse, Am. Compl. ¶ 92 n.83; Treasury has made disclosures in connection with the halting of already-approved disbursements, *id.* ¶ 64 n.47; and Education has made the disclosures in connection with efforts to terminate its own existence, *id.* ¶ 116 n.104. These uses are a far cry from the mission-critical "routine uses" promulgated by Defendants and do not align with the purposes for which the records were collected. *See, e.g.*, Martinez Decl. ¶ 10 (DOGE representatives "appear to be using [my personal data] for purposes that have nothing to do with why I provided the data.").

Nor are Defendants permitted to twist the meaning of existing "routine uses" to shoehorn in their impermissible disclosures. An agency "may not utilize the 'routine use' exception to circumvent the mandates of the Privacy Act" by promulgating purported "routine uses" that are not, in fact, compatible with the purpose for which the agency collected the records at issue, as required by the Act. *Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988). This is equally true where an agency adopts a strained interpretation of a promulgated "routine use" in an effort to rationalize a disclosure post-hoc. *See id.* Defendants' publicly documented explanations for

their disclosures make clear that they were not made in accordance with the requirement of the statute; no amount of massaging the language of their "routine use" exemptions can change that.

Defendants' decision to grant DOGE representative sweeping access to government data systems containing sensitive PII without Plaintiffs' consent is clearly contrary to the Privacy Act and exceeds the boundaries of Defendants' statutory authority to disclose under that Act.

2. Defendants' Decisions to Disclose Were Arbitrary and Capricious

Defendants' decisions to grant access to secured records systems were arbitrary and capricious. Agency actions are arbitrary where an agency fails to "consider an important aspect of the problem," *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983), or otherwise engage in "reasoned decision making." *Michigan v. EPA*, 576 U.S. 743, 750 (2015) (citation omitted). Here, Defendants' decision to grant access to DOGE officials manifestly failed to consider a critical aspect of the problem at hand: the security risks associated with allowing such sweeping access to sensitive personally identifying information belonging to tens of millions of Americans, including Plaintiffs. Specifically, Defendants failed to properly vet officials receiving the records or install security precautions commensurate with the sensitivity of the information at issue—namely, information that could readily facilitate identify theft and other economic crimes against millions of Americans, *see Bohnak v. Marsh & McLennan Co.*, 79 F.4th 276, 287 (2d Cir. 2023) (exposure of PII to "malignant" outside actor gave rise to a substantial risk of future identity theft or fraud). As a result, they have placed that information in the hands of a core group of DOGE employees, which includes a teenager who was recently fired from a corporate internship for allegedly leaking sensitive information to a competitor. Am. Compl. ¶ 37 n.10, 138 n.124.

Underscoring Defendants' arbitrary decision making in this instance is the fact that Treasury recently conducted an internal threat analysis that designated DOGE as an "insider threat" and characterized DOGE's administrative access to the Treasury's payment systems as "the single greatest insider threat risk the Bureau of the Fiscal Service has ever faced." *See id.*

¶ 135 n.118. That same intelligence report recommended *immediately* suspending DOGE's access. *Id.* Prior to these disclosures, it had been "extremely unusual" for individuals connected to political appointees to request, much less gain access to, FDS payment systems. *Id.* ¶ 48 n.25. Notwithstanding this, Treasury and the other agency Defendants have not meaningfully restricted DOGE's access. This outcome betrays a complete absence of the "reasoned decision making" required by the APA and instead smacks of capriciousness. *See Roe v. Dep't of Def.*, 947 F.3d 207, 228 (4th Cir. 2020) (agency action likely to be held arbitrary and capricious where it "evidences a complete failure to reasonably reflect upon the information contained in the record and grabble with contrary evidence—disregarding entirely the need for reasoned decision-making").

II. Plaintiffs Will Suffer Immediate, Irreparable Harm If an Injunction Does Not Issue.

Defendants' ongoing and unauthorized disclosure of Plaintiffs' sensitive, personally identifiable information to DOGE representatives has harmed and will continue to irreparably harm Plaintiffs. "To establish irreparable harm, the movant must make a 'clear showing' that it will suffer harm that is 'neither remote nor speculative, but actual and imminent.'" *Mountain Valley Pipeline, LLC v. 6.56 Acres of Land*, 915 F.3d 197, 216 (4th Cir. 2019) (citation omitted). "Additionally, the harm must be irreparable, meaning that it 'cannot be fully rectified by the final judgment after trial.'" *Id.* (quoting *Stuller, Inc. v. Steak N Shake Enters.*, 695 F.3d 676, 680 (7th Cir. 2012).

Plaintiffs easily satisfy both requirements. Defendants have unlawfully granted dozens of DOGE representatives sweeping access to Plaintiffs' PII across multiple systems. As discussed *supra* pp 4-9, that includes disclosure of Plaintiffs' social security numbers, addresses, birth dates, immigration status, income, driver's license information, and contact information. *E.g.*, Martinez Decl. ¶ 8. Much of this information is so sensitive that the Federal Rules of Civil Procedure require litigants to redact them in any federal court proceeding. *See* Fed. R. Civ. P. 5.2(a). That is unsurprising. "Courts consistently recognize that PII can be used to commit

identity theft." *In re Marriott Int'l Customer Data Sec. Breach Litig.*, 2022 WL 951692, at *5 (D. Md. Mar. 30, 2022), *R. & R. adopted by In re Marriott*, No. 8:18-MD-02879, ECF No. 1005; *see* Martinez Decl. ¶ 11 ("I am worried that unauthorized access and disclosure of my personal information held within the federal government will compromise my personal safety and security."). Defendants' disclosure of Plaintiffs' PII is "neither remote nor speculative." *Mountain Valley Pipeline*, 915 F.3d at 216. To the contrary, disclosure of Plaintiffs' PII is active and ongoing, and appears likely to be disclosed to additional DOGE representatives and/or AI tools or software absent this Court's intervention.

The harm Plaintiffs have suffered, and will continue to suffer, from the unlawful disclosure of their PII to DOGE representatives is also irreparable. The Privacy Act was intended to protect the individual right to privacy, *supra* pp 3-4. Left unchecked, Defendants will continue to run roughshod over Plaintiffs' right to privacy. That is the "quintessential type" of irreparable harm that preliminary injunctive relief is intended to prevent, because the violation is both "substantial and irreversible." *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000); *see also In re Alrich Pump, LLC*, 2023 WL 3108509, at *2 (W.D.N.C. Apr. 26, 2023).

In this case, the disclosure of sensitive financial and personal information "is a bell that one cannot unring." *Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 755 (D. Md. 2012). Without an injunction, Defendants will provide increasing numbers of DOGE representatives with access to Plaintiffs' sensitive information; and DOGE representatives who already have access to these systems will remain at liberty to make unauthorized copies of that data and also to feed Plaintiffs' sensitive PII into AI systems. Each additional disclosure is an act of irreparable harm that compounds Defendants' violations of Plaintiffs' privacy rights. And as a practical matter, the longer DOGE representatives are able to maintain their access to these sensitive data systems, the greater the risk to Plaintiffs that this information will be disclosed by those DOGE representatives to yet more individuals or even outside the government through the use of AI tools and software to potentially devastating effect.

These harms have not been ameliorated by the orders issued in *Alliance for Retired Americans v. Bessent*, No. 1:25-cv-00212 (D.D.C.) and *New York v. Trump*, No. 1:25-cv-01144 (S.D.N.Y.), because those orders address only Defendants' disclosure of FDS records to DOGE. They also are not resolved by the stipulation Education entered into in *Univ. of Cal. Student Ass'n v. Denise Carter*, No. 1:25-cv-00354 (D.D.C. Feb. 11, 2025), which lasts only until February 17, and does not require Education to retrieve and destroy copies of records disclosed to DOGE representatives. *See id.* ECF No. 12. As of the date of this filing, DOGE representatives can continue to access Plaintiffs' sensitive records maintained by OPM, including making local copies of those records, sharing records with other members of DOGE who do not themselves have access to the systems, and/or feeding Plaintiffs' PII into AI tools and software; and DOGE representatives can continue to hold onto any copies of PII retrieved from Education. Longstanding principles of equity do not require Plaintiffs to stand by helplessly while DOGE representatives plunder their personal and private information in violation of the law. Because Plaintiffs are suffering ongoing irreparable harm, this Court is empowered to issue preliminary injunctive relief to prevent further harm. *See, e.g.*, *Hisp. Nat'l L. Enf't Ass'n NCR v. Prince George's County*, 535 F. Supp. 3d 393, 427 (D. Md. 2021) (issuing preliminary injunction after finding "irreparable harm from the ongoing effects" of the government's conduct).

III. The Equities and Public Interest Favor a Temporary Restraining Order.

The remaining factors also weigh in favor of a restraining order to preserve the status quo and protect Plaintiffs' sensitive information. Plaintiffs must show "the balance of equities tips in [their] favor, and that an injunction is in the public interest." *Winter* , 555 U.S. at 20. These "merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009). Here, a restraining order will serve the public interest by enforcing and protecting the privacy rights codified by the Privacy Act. "[T]he public 'undoubtedly has an interest in seeing its governmental institutions follow the law.'" *Vitkus v. Blinken*, 79 F.4th 352, 368 (4th Cir. 2023) (citation omitted); *see also Sanchez v. McAleenan*, 2024 WL 1256264, at *14 (D. Md. Mar. 25, 2024) ("[Government] Defendants 'cannot suffer harm from an injunction that merely ends an

unlawful practice.'" (citation omitted)). The Privacy Act of 1974 was enacted by Congress to "restore trust in government and to address what at the time was seen as an existential threat to American democracy." Off. of Priv. & Civ. Liberties, *Overview of the Privacy Act of 1974: 2020 Edition*, at 1, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction. A restraining order here will serve the public's interest by giving effect to a law of "fundamental importance." *See* Privacy Act Legis. Hist. at vii.

The peril of irreversible private-data exposure faced by Plaintiffs—and the public—also far eclipses any interest the Government might have in pursuing its agenda to disrupt routine federal agency operations. Indeed, President Trump recently acknowledged that DOGE has no need for access to Plaintiffs' personal information, indicating the Government will suffer no harm whatsoever from a temporary restraining order protecting that information. *See* White House, *President Trump Holds a Press Conference with Prime Minister Shigeru Ishiba of Japan*, YouTube, at 15:42–16:31 (Feb. 7, 2025), https://www.youtube.com/live/jMiAE9X-Wig?si=S0NkrDwEwLbrvTYM&t=942 ("[Reporter:] DOGE engineers have access to . . . . American's personal information like social security numbers, home addresses, bank accounts—why does DOGE need all of that stuff? [President:] Well, it doesn't, but they get it very easily.").

Absent a restraining order, Defendants will continue to grant DOGE representatives access to Plaintiffs' sensitive PII in their systems, without regard for how Plaintiffs' data is used, copied, or further shared, and in violation of their privacy rights. The government, in contrast, "will suffer only a delay in implementation" of its new (less protective) data-access policies and decisions if it is ultimately successful on the merits. *Mayor & City Council of Baltimore v. Azar*, 392 F. Supp. 3d 602, 619 (D. Md. 2019); *see Senior Execs. Ass'n*, 891 F. Supp. at 753, 755 (concluding irreparable harm from potential disclosure of sensitive financial data "overwhelmingly" outweighed government's interest in "deterring corruption"). The balance of equities and public interest decisively weigh in favor of issuing a temporary retaining order to prevent further unauthorized access to Defendants' data systems.

CONCLUSION

For the foregoing reasons, the Court should enter a temporary restraining order in the form requested by Plaintiffs.

DATED: February 12, 2025

By: */s/Xiaonan April Hu*
(signed by filer with permission)

Xiaonan April Hu (*pro hac* pending)
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW
Washington, DC 20001
(202) 220-1123
April.Hu@mto.com

John L. Schwab (*pro hac* pending)
MUNGER, TOLLES & OLSON LLP
350 S Grand Ave 50th Floor
Los Angeles, California 90071
(213) 683-9260
John.Schwab@mto.com

Carson Scott (*pro hac* pending)
Roman Leal (*pro hac* pending)
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty-Seventh Floor
San Francisco, California 94105-2907
(415) 512-4000
Carson.Scott@mto.com
Roman.Leal@mto.com

/s/ Mark Hanna

Mark Hanna (Fed. Bar No. 16031)
David J. Rodwin (Fed. Bar No. 18615)
MURPHY ANDERSON PLLC
1401 K Street NW, Suite 300
Washington, DC 20005
T: (202) 223-2620 | F: (202) 296-9600
mhanna@murphypllc.com
drodwin@murphypllc.com

Daniel McNeil (*pro hac* pending)
General Counsel
American Federation of Teachers, AFL-CIO
555 New Jersey Ave. NW
Washington, DC 20001
T: (202) 393-6305 | F: (202) 393-6385
dmcneil@aft.org

Kristy Parker (*pro hac* pending)
Jane Bentrott (*pro hac* pending)
Shalini Goel Agarwal (*pro hac* pending)
PROTECT DEMOCRACY PROJECT
2020 Pennsylvania Ave. NW, Suite 163
Washington, DC 20006
202-843-3092
kristy.parker@protectdemocracy.org
jane.bentrott@protectdemocracy.org
shalini.agarwal@protectdemocracy.org

Benjamin L. Berwick (*pro hac* forthcoming)
PROTECT DEMOCRACY PROJECT
15 Main Street, Suite 312
Watertown, MA 02472
(202) 579-4582
ben.berwick@protectdemocracy.org

Jessica A. Marsden (*pro hac* pending)
PROTECT DEMOCRACY PROJECT
510 Meadowmont Village Circle, No. 328
Chapel Hill, NC 27517
(202) 579-4582
jess.marsden@protectdemocracy.org

Laurence M. Schwartztol (*pro hac* pending)
DEMOCRACY AND RULE OF LAW CLINIC
Harvard Law School
1525 Massachusetts Avenue
Cambridge, MA 02138
(617) 998-1877
lschwartztol@law.harvard.edu

Attorneys for Plaintiffs