

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

State of New York, *et al.*

Plaintiffs,

v.

Case No. 1:25-cv-1144-JAV

U.S. Department of the Treasury, *et. al.*

Defendants.

I, Joseph Gioeli III, declare under penalty of perjury:

1. I currently serve as the Deputy Commissioner for Transformation and Modernization in the Bureau of the Fiscal Service (Bureau or BFS), in the U.S. Department of the Treasury (Treasury), and have been employed in this role since 2023. I report to the Commissioner of the Bureau. I am a career civil servant. Prior to my current position, I also served as the Bureau's Chief Technology Officer from 2017-2020 and its Chief Information Officer from 2020-2023. I have been employed at the Bureau for over seven years.
2. In my current role, I oversee, among other things, the Bureau's Office of Information and Security Services (ISS). ISS promotes the integrity and operational efficiency of the federal government's financial infrastructure that is within Treasury's responsibility, while ensuring the security of that infrastructure and the information it contains. In my position, I oversee the Chief Information Officer, who has authority over the security of and access to these systems. I have extensive knowledge of the Bureau's technology investments, as well as the related technology and cybersecurity strategies that support our enterprises.

3. I also understand the security posture of these systems, the types of data that generally transact through these systems, and their criticality to the national critical infrastructure. I am also familiar with Bureau requirements around access to sensitive systems.
4. In my current role, I have been involved in the Bureau's efforts to develop and implement a 4- to 6-week payment process engagement plan ("engagement") in which the Bureau would support Treasury employees from the Treasury DOGE Team in understanding payment processes and identifying opportunities to advance payment integrity and fraud reduction goals. The Treasury DOGE Team involved in this engagement consisted of Thomas Krause and Marko Elez. To date, to the best of my knowledge, Mr. Elez has been the only individual on the Treasury DOGE Team who has been provided direct access to BFS payment systems or source code. Mr. Krause had "over the shoulder" access by which he could view BFS payment systems or source code while they were being accessed by another person with the required access and permissions. I understand that Mr. Elez had provided Mr. Krause with updates about his work, which may have occasionally included screenshots of payment systems data or records, but Mr. Krause did not receive direct access to BFS payment systems or source code.
5. BFS has multiple payment and accounting systems that are responsible for different tasks and processes, which are involved in BFS's engagement with the DOGE team. These include Payment Automation Manager (PAM), Secure Payment System (SPS), Automated Standard Application for Payments (ASAP), International Treasury Services (ITS.gov), and the Central Accounting and Reporting System (CARS).
6. PAM is the primary application used by Treasury to process payments for disbursement, and it includes several components. PAM's "file system" is where payment files are transferred

from initiating agencies before processing and certification, sometimes referred to as its “landing zone.” Once certified by the initiating agency certifying official, PAM’s “payment processing system” processes the payments consistent with the instructions within the file. The PAM payment process is described in more detail in the accompanying declaration of Vona S. Robinson.

7. ASAP is a recipient-initiated electronic payment and information system; this means that it is a payment system that allows recipients to draw down funds from an established account for that recipient.
8. SPS is a system through which paying agencies securely create, certify, and submit individual payment files to Treasury; it is also typically used for one-time large dollar amount transactions.
9. International Treasury Services.gov (ITS) allows federal agencies to make international payments, which are often used, for example, to provide Social Security benefit payments to Americans living abroad.
10. Finally, the Central Accounting and Reporting System (CARS) is the electronic system for recording the federal government’s financial data on an agency’s spending and provides streamlined agency reporting for accounting purposes.
11. The scope of work as envisioned in the engagement plan required access to Fiscal Service source code, applications, and databases across all these Fiscal Service payment and accounting systems and their hosting environments. This broad access presented risks, which included potential operational disruptions to Fiscal Service’s payment systems, access to sensitive data elements, insider threat risk, and other risks that are inherent to any user access

to sensitive IT systems. In light of these risks, BFS and Treasury Departmental Office employees developed mitigation strategies that sought to reduce these risks.

12. These measures included the requirement that Mr. Elez be provided with a BFS laptop, which would be his only method of connecting to the Treasury payments systems, both in connecting with the source code repository and for his read-only access of the systems. He had previously been provided a Treasury laptop from the Department shortly after he onboarded, but due to Bureau security policy, that device was restricted from accessing the BFS systems and services he had requested. BFS used several cybersecurity tools to monitor Mr. Elez's usage of his BFS laptop at all times and continuously log his activity. Additionally, the Bureau enabled enhanced monitoring on his laptop, which included the ability to monitor and block website access, block the use of external peripherals (such as USB drives or mass storage devices), monitor any scripts or commands executed on the device, and block access to cloud-based storage services. Additionally, the device contained data exfiltration detection, which alerts the Bureau to attempts to transmit sensitive data types. The laptop is also encrypted in accordance with Bureau policy, which, if the laptop were stolen or lost, would prevent unauthorized users from accessing data contained within the laptop.

13. Additional mitigation measures that were adopted included that Mr. Elez would receive "read-only" access to the systems, and that any reviews conducted using the "read-only" access would occur during low-utilization time periods, to minimize the possibility of operational disruptions. While providing a single individual with access to multiple systems and data records accessed here was broader in scope than what has occurred in the past, this read-only approach is similar to the kind of limited access the Bureau has provided to

auditors for other Treasury non-payment systems, though even in those scenarios the availability of production data was significantly limited.

14. Further, it was agreed that in the near-term only a single Treasury employee, Mr. Elez, would be designated as the “technical team member” who would exercise this read-only access. The Bureau would provide safeguarding and handling instructions for Treasury data for the duration of the project, and ISS personnel instructed Mr. Elez and Mr. Krause that no Treasury information and data could leave the Bureau laptop for the duration of the engagement, consistent with what was outlined in the engagement plan. The Treasury DOGE Team also agreed that, at the end of the project, it would provide the Bureau with an attestation statement that any copies of Treasury information made would be properly destroyed, and confirmation that no suspicious or unauthorized access to Bureau information or data had occurred during the engagement.
15. Overall, BFS and Treasury leadership were fully aware of the risks presented by Mr. Elez’s work and sought to mitigate those risks to the extent possible through the measures just described.
16. On January 28, 2025, the Bureau provided Mr. Elez with the Bureau laptop and with copies of the source code for PAM, SPS, and ASAP in a separate, secure coding environment known as a “secure code repository” or “sandbox.” Mr. Elez could review and make changes locally to copies of the source code in the cordoned-off code repository; however, he did not have the authority or capability to publish any code changes to the production system or underlying test environments. This repository was separate from Fiscal Service’s typical code development environment, and unlike the usual code development environment, this

new repository was segmented, to ensure that no changes to the operative source code could be made.

17. On February 3, 2025, consistent with the engagement plan and mitigation measures developed, Mr. Elez was provided with read-only access, through his Bureau laptop, to the certain BFS systems. The read-only access that Mr. Elez was provided gives the user the ability to view and query information and data but does not allow for any changes to that information and data within its source system. While this reduces risk, it does not fully eliminate the risks identified in the assessment (for example, the risk of overburdening the system with a complex read-only query). Specifically, Mr. Elez was provided read-only access to the Payment Automation Manager (PAM) Database, Payment Automation Manager (PAM) File System, and, subsequently on February 5, the Secure Payment System (SPS) Database.
18. ISS configured his network access and assisted him in setting up the necessary tools to connect to the PAM database on February 3. His access was closely monitored by multiple BFS administrators throughout the process on February 3. That same day, he received a “walk-through” demonstration of two BFS payment systems, the PAM database and the PAM file system (the system that controls the payment file “landing zone” discussed above), to see how the systems worked. He logged in with his read-only access to these systems on February 3 during this “walk-through” demonstration. The Bureau is in the process of reviewing the logs of Mr. Elez’s activity on his Bureau laptop, and this review remains ongoing. Based on the preliminary log reviews conducted to date, it appears that on February 3, Mr. Elez copied two USAID files directly from the PAM database to his BFS laptop; on February 4 and 5, Mr. Elez accessed the PAM file system; and on February 5, Mr. Elez

accessed the PAM payment processing database. These activities are consistent with the read-only access that Mr. Elez was provided and did not change or alter any BFS payment system or record within their source systems. As noted, reviews of Mr. Elez's work are still actively occurring; I do not have any more detail to provide at this time about his activities with respect to PAM.

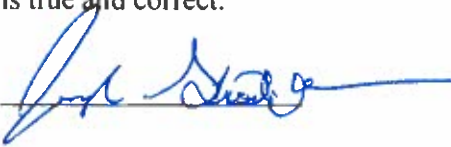
19. Due to scheduling constraints, Mr. Elez was unable to meet with Bureau personnel to set up his access to the SPS database until February 5. On that date, ISS held a virtual walk-through session to help him to connect to the SPS database. He accessed this database exclusively under the supervision of Bureau database administrators in a virtual walkthrough session. According to the preliminary review of logs the Bureau has conducted to date, it appears Mr. Elez accessed the SPS database only once during that walk-through demonstration on February 5. It does not appear that he accessed the database again. As part of the ongoing review, additional log reviews are currently underway to confirm this. Mr. Elez never logged into ASAP, CARS, or ITS.gov, as technical access to those systems was never established for him.
20. On the morning of February 6, it was discovered that Mr. Elez's database access to SPS on February 5 had mistakenly been configured with read/write permissions instead of read-only. A forensic investigation was immediately initiated by database administrators to review all activities performed on that server and database. The initial investigation confirmed that all of Mr. Elez's interactions with the SPS system occurred within the supervised, walk-through session and that no unauthorized actions had taken place. His access was promptly corrected to read-only, and he did not log into the system again after his initial virtual over-the-shoulder session on February 5. To the best of our knowledge, Mr. Elez never knew of the

fact that he briefly had read/write permissions for the SPS database, and never took any action to exercise the “write” privileges in order to modify anything within the SPS database—indeed, he never logged in during the time that he had read/write privileges, other than during the virtual walk-through – and forensic analysis is currently underway to confirm this.

21. As noted above, the Bureau used several cybersecurity tools to monitor Mr. Elez’s usage and continuously log his activity. While forensic analysis is still ongoing, Bureau personnel have conducted preliminary reviews of logs of his activity both on his laptop and within the systems and at this time have found no indication of any unauthorized use, of any use outside the scope that was directed by Treasury leadership, or that Mr. Elez used his BFS laptop to share any BFS payment systems data outside the U.S. Government.
22. On February 6, 2025, Mr. Elez submitted his resignation as a Treasury employee. After the Bureau received written notification from the Department confirming his resignation, it revoked or removed all physical and logical access and recovered all Treasury equipment, including his Treasury Departmental Offices and Bureau laptops, Treasury Departmental Offices government cell phone, and Treasury building access cards.
23. I have consulted with other BFS officials familiar with our access policies, and to date we have not identified any BFS policies (in effect either currently or prior to January 20, 2025) that disallow Federal employees from accessing the BFS payment and accounting systems identified above on the basis that they hold non-career (or political) appointments or are Special Government Employees.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 2/11/25

Signed: 

Joseph Gioeli III
Deputy Commissioner of Transformation and
Modernization
Bureau of the Fiscal Service
United States Department of the Treasury

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

State of New York, *et al.*

Plaintiffs,

v.

Case No. 1:25-cv-1144-JAV

U.S. Department of the Treasury, *et. al.*

Defendants.

I, Vona S. Robinson, declare under penalty of perjury:

1. I currently serve as the Deputy Assistant Commissioner for Federal Disbursement Services at the Bureau of the Fiscal Service (BFS or the Bureau). I have been employed in this role since October 2022; prior to that, I served as Executive Director Federal Disbursement Services from February 2019 to October 2022. I report to Linda Chero, Assistant Commissioner, Disbursing and Debt Management. I am a career civil servant.
2. In my current role, I oversee, among other things, the Bureau's Federal Payment Operations. My office is responsible for disbursing 87.8% of the U.S. Government's payments valued at 5.46 trillion dollars annually. My office works closely with BFS's Office of Transformation and Modernization, which is headed by Deputy Commissioner Joseph Gioeli. Mr. Gioeli's office is responsible for the integrity, operational efficiency, and security of the technological infrastructure, whereas the Office for Disbursement Services is responsible for overseeing the business processing of payment requests that come into BFS's payment systems.

3. In this role, I have extensive knowledge of the Fiscal Service business processes for the disbursement of federal payments. Information in this declaration is based on my personal knowledge and information made available to me in the course of my official duties. I provide this declaration in support of Defendants' opposition to Plaintiffs' Motion for a Temporary Restraining Order in the above-captioned case.
4. As described in the accompanying Declaration of Joseph Gioeli, BFS has multiple payment systems that are responsible for different tasks and processes; multiple of these systems are involved in BFS's engagement with the Treasury Department of Government Efficiency (DOGE) team. As relevant to the topics discussed in this declaration, Payment Automation Manager (PAM) is the primary application used by Treasury to process payments for disbursement, and it includes several component sub-systems, as discussed below. Secure Payment System (SPS) is another payment processing system, through which agencies securely create, certify, and submit payment files to Treasury; it is also typically used for one-time large dollar amount transactions.
5. Within PAM, PAM's "file system" receives payment files from payor agencies into its "landing zone," which is the existing system that ingests payment files before agencies certify the payments for processing. When payment files come into the "landing zone," they are transferred to the PAM application where the payment file is validated and a pre-edit report is generated and sent back to the Federal Agency that contains, among other things, information about potentially improper or fraudulent payments. The Federal Agency uses this report to certify the payments in the SPS system, after which the payments are processed consistent with the instructions within the file.

6. I am familiar with the Bureau's efforts to develop and implement a 4-6 week payment process engagement plan ("engagement") in which the Bureau would support the Treasury DOGE Team—which I understand consisted of Tom Krause and Marko Elez, until Mr. Elez's resignation on February 6, 2025. I understand that the purpose of the engagement was to understand BFS payment processes and identify opportunities to advance payment integrity and fraud reduction goals.
7. I am also aware of Treasury leadership's decision to approve a process that would assist agencies in complying with the President's January 20, 2025 Executive Orders requiring that certain types of foreign aid-related payments be paused, and I am familiar with the Treasury DOGE Team's collaboration with BFS staff, including some within my office, to help effectuate this decision.
8. I understand that, on or about January 26, 2025, Treasury leadership approved a process that would assist agencies in complying with the President's January 20, 2025 Executive Order on foreign aid. Specifically, the Bureau was directed to develop a process to identify all USAID payment files within the PAM file system's "landing zone," to flag those payments for the State Department as potentially implicated by the President's foreign aid Executive Order, prior to their entry into the PAM payment processing systems. Before this process could get fully underway, however, on January 27, Treasury leadership informed BFS that State Department had decided to intercept the USAID files prior to the initial submission to BFS, and therefore it would not be necessary to continue

to flag any USAID payment files for the State Department's review. Between January 26 and the revised decision on January 27, BFS did not receive any USAID payment files.¹

9. On January 27, 2025, the Bureau of Information and Security Services (ISS), a component of BFS, established the secure portal that would allow the authorized State Department officials to retrieve copies of the identified payment files consistent with the authorized process.
10. On January 31, the Bureau was directed to (1) identify incoming specific Agency payment files to the "landing zone" that met 4 specified Treasury Account Symbol (TAS)² codes,—I understand that those TAS codes had been associated with categories of payments that were not USAID payments, but which nonetheless may have been covered under the foreign aid Executive Order; (2) create a copy of the payment files with those TAS codes—the original payment files would remain in the landing zone to ensure payment integrity; (3) move those copies into a separate folder (the "MoveIT" folder) where they could be sent to authorized officials at the State Department for review; (4) deliver the copies to authorized staff at the State Department through a secure portal that was limited in access to certain designated Department of State officials, for same-day

¹ Several USAID payment files *were* received later, on February 4 and February 5—BFS received a separate authorization email from the USAID copying State Department indicating that the files should move forward as scheduled, which they did. No USAID payment files were received after February 5.

² A TAS is an identifier for a particular agency's account, which typically is associated with an individual agency appropriation, receipt, or other fund account. One TAS code was associated with the Millennium Challenge Corporation (MCC) and three TAS codes were associated with certain payments from the Department of Health and Human Services (HHS). These included two sub-accounts labeled "Refugee and Entrant Assistance, Admin for Children and Families," one account labeled "Gifts and Donations Office of Refugee Resettlement, Admin for Children and Families," and one account labeled "Refugee Resettlement Assistance, Administration for Children and Families, Health and Human Services."

review, and (5) allow those State Department officials to determine whether the Executive Order required a pause, or whether the original payment files should move forward into PAM's processing system for disbursement according to Treasury's normal payment processes.

11. At the outset, I understand that BFS career staff queried the PAM file system manually to identify payment files and shared those payment files with Mr. Elez for review through the MoveIT folder. I further understand that, at some point after January 31, Mr. Elez assisted in automating the manual review of the payment files.
12. On the afternoon of February 6, 2025, Mr. Elez resigned, and his electronic devices were returned to BFS and the Treasury Department.
13. On the morning of February 7, four payment files were flagged with a TAS associated with the "Refugee and Entrant Assistance, Admin for Children and Families" account, indicating that the State Department review should be conducted. At 2 p.m., the State Department indicated that the files could be processed normally, as the State Department determined it did not have authority over the payments under the Executive Order. The four payment files were then processed in the normal course that same day.
14. On February 10, Millennium Challenge Corporation submitted an international payment request. The payment was forwarded to State Department for further review consistent with the established process. At approximately 2:00 pm eastern, the MCC certifying official (not the State Department representative) requested Fiscal Service to not process the payment.

15. As of February 10, we have ensured that the State Department review process will not proceed for payment requests within the scope of the TRO order issued in *New York v. Trump*, No. 1:25-cv-39-JJM-PAS (D.R.I.).
16. To the best of my knowledge, BFS has not failed to disburse any payment duly certified by a payor agency as a result of the Treasury DOGE Team's work. To date, no payments, with the exception of the single MCC payment mentioned above, have been delayed or canceled by the payor agency as a result of the re-routing and review process described herein.

I swear upon penalty of perjury that the foregoing is true and correct.

Dated: 2/11/2025

Vona S. Robinson

Vona S. Robinson

Deputy Assistant Commissioner – Federal
Disbursement Services

Bureau of the Fiscal Service

U.S. Department of the Treasury

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

State of New York, *et al.*

Plaintiffs,

v.

Case No. 1:25-cv-1144-JAV

U.S. Department of the Treasury, *et. al.*

Defendants.

I, Thomas H. Krause, Jr., declare under penalty of perjury:

1. I am employed as the Senior Advisor for Technology and Modernization at the Department of the Treasury. I started serving in this role on January 23, 2025. This role is currently unpaid, and I am not seeking compensation, as permissible by law. I am also designated as a Special Government Employee (SGE). While in this Treasury role, I have also maintained my employment as Chief Executive Officer (CEO) of Cloud Software Group, Inc., which is a privately held company comprised of several enterprise software businesses. Treasury's ethics office determined, based on my role as an SGE, that this arrangement was permissible. In addition to serving as Senior Advisor for Technology and Modernization, on February 5, 2025, the Treasury Secretary delegated the performance of duties of the Fiscal Assistant Secretary to me, although I have not yet assumed those duties.
2. My role at Treasury as Senior Advisor for Technology and Modernization was created to help effectuate the mission of the President's Department of Government Efficiency (DOGE). Under the President's January 20, 2025 Executive Order establishing the U.S. DOGE Service (USDS/DOGE) as a temporary organization within the Executive Office of the President that

seeks to maximize governmental efficiency and productivity, the President directed each Agency Head to establish a DOGE team of at least four employees, which may include Special Government Employees, within 30 days. In this role, I am responsible, among other duties, for reducing and eliminating improper and fraudulent payments; waste, fraud, and abuse; and improving the accuracy of financial reporting. To that end, I am focused on improving the controls, processes, and systems that facilitate payments and enable consolidated financial reporting. I serve as the DOGE team lead for the Treasury Department (Treasury DOGE Team).

3. Currently, I am the only Treasury DOGE team member. A second Treasury DOGE team member, Marko Elez, began working at the Treasury Department on January 21, 2025, but resigned from his role on February 6, 2025. Marko Elez is a highly qualified software engineer who previously worked at several of Elon Musk's companies, including SpaceX and X (formerly Twitter). In January, USDS/DOGE recommended to me, and to incoming Treasury leadership, that Mr. Elez be selected as the Treasury DOGE Team's technical team member. Treasury hired Mr. Elez as a Special Advisor for Information Technology and Management. In this role, Mr. Elez was a Treasury employee tasked with working closely with engineers at the Bureau of the Fiscal Service (BFS) on information technology (IT) matters in service of BFS's mission to promote financial integrity and operational efficiency of the federal government through accounting, financing, collection, payment, and other relevant BFS services. On February 6, 2025, Mr. Elez submitted his resignation from this role. On that same day, he turned in his Treasury laptop, BFS laptop, access card, and other government devices; his BFS systems access was terminated; and he has not conducted any work related to the BFS payment systems since that date.

4. Although I coordinate with officials at USDS/DOGE, provide them with regular updates on the team's progress, and receive high-level policy direction from them, I am not an employee of USDS/DOGE. My role on the Treasury DOGE Team is to find ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of this Administration.
5. Although I have not yet assumed the duties of the Fiscal Assistant Secretary, in this role, I will be the official primarily responsible for overseeing the activities of the Bureau of the Fiscal Service (BFS), which manages the government's accounting, central payment systems, and public debt, among other tasks, and which serves as the central payment clearinghouse for all payments to and from federal agencies. BFS is responsible for disbursing the majority of U.S. Government payments, valued at more than \$5 trillion annually.
6. I bring to my work at Treasury a wealth of experience from my long and successful business career in the technology industry, helping make major software enterprises more efficient, effective, innovative, and profitable. As noted above, I am currently the CEO of Cloud Software Group, one of the largest privately held enterprise software companies globally. Over the last two years, we have dramatically improved the company's effectiveness and efficiency by, among other things, improving our business processes and integrating and modernizing our technology systems. Prior to my employment at Cloud Software Group, I spent over a decade at Broadcom, where I was an executive officer serving as CFO and most recently as President of Broadcom Software. Broadcom is one of the most valuable companies in the world today and was built largely by acquiring underperforming semiconductor and enterprise software businesses and improving their effectiveness and efficiency. I am proud of this work, and I bring this focus on effectiveness and efficiency to

my work for the Treasury Department and in service of the President’s DOGE mission, to help maximize value for the American taxpayer and make our Government better for future generations.

7. As illustrated by several reports released by the Government Accountability Office (GAO), we have our work cut out for us. On January 16, 2025, GAO released a report entitled “Financial Audit: FY2024 and FY2023 Consolidated Financial Statements of the U.S. Government.” In the report, GAO summarizes that they were not able to determine if the Financial Report of the U.S. Government is fairly presented. Among other reasons, GAO highlighted “problems in accounting for transactions between federal agencies.” GAO found many material weaknesses including “the federal government’s inability to determine the full extent to which improper payments, including fraud, occur and reasonably assure that appropriate actions are taken to reduce them.” GAO also reported that Treasury and Office of Management and Budget (OMB) officials expressed their continuing commitment to addressing the problems this report outlines. In short, the GAO report identifies the Federal government’s inability to account for all of the improper payments including waste, fraud and abuse across federal agencies.
8. On September 10, 2024, the GAO released a report entitled “Payment Integrity: Significant Improvements are Needed to Address Improper Payments and Fraud.” The report found that since 2003, cumulative improper payments¹ by executive branch agencies have totaled about \$2.7 trillion dollars. Some of GAO’s top concerns included fraudulent or improper Earned Income Tax Credit refunds, Social Security payments, unemployment insurance payments,

¹ Improper payments and fraudulent payments are related but distinct concepts. An improper payment is a payment that should not have been made, or that was made with an incorrect amount; fraudulent payments occur due to willful misrepresentation. All fraudulent payments are improper, but not all improper payments are fraudulent.

and Medicare and Medicaid payments. In fiscal year 2023 alone, federal agencies estimated \$236 billion in improper payments across more than 70 federal programs. In addition, GAO estimated that the total annual financial losses across the government from fraud are between \$233 and \$521 billion. These numbers are truly staggering—billions and billions in hard-earned American taxpayer dollars are being misspent every year. GAO highlighted a number of steps that Congress and federal agencies could take to help reduce fraud and improper payments, including that “[a]gencies should improve oversight to ensure that funds aren’t paid to ineligible recipients” and that “[a]gencies should improve their collection and use of data for preventing and detecting fraud.”

9. Similarly, GAO has identified areas for improvement in BFS’s systems related to identifying and tracing transactions to determine whether they were complete and properly recorded in the correct general ledger accounts and line items within the Schedules of the General Fund. *See* GAO Report, “Financial Statement Audit: Bureau of the Fiscal Service’s FY22 Schedules of the General Fund” (March 30, 2023). Specifically, GAO has found inconsistent reporting, lack of traceability, and need for improved controls with the Treasury’s Central Accounting and Reporting System (CARS), which federal agencies use to track their spending for budgetary and accounting purposes. These kinds of improvements and others can enhance BFS’s ability to ensure accountability in the spending of taxpayer dollars.
10. BFS is well positioned to help agencies and the federal government holistically understand and take stock of the problems GAO has reported on, and assist agencies in the government-wide mission to stop fraudulent and improper payments, including by enhancing our ability to help agencies identify payments that may potentially be directed to fraudulent accounts, payments to individuals or entities which may be barred from receiving government

payments, payments that are potentially improperly sent to deceased individuals, may have a mismatch between payee and account data, or have other indicators of problems.

11. For this reason, an important aspect of the President's DOGE efforts has been to quickly place me into the Treasury Department so I can understand how BFS's end-to-end payment systems and financial report tools work, recommend ways to update and modernize those systems to better identify potentially improper and fraudulent payments, and find ways for BFS to assist federal agencies in responding to statutes, regulations, and Executive Orders that affect the Government's payment authorities and spending priorities.
12. As soon as I arrived at the Treasury Department, I met with Treasury leadership to begin operationalizing the Treasury DOGE Team's work. This early work included: (1) initiating conversations with BFS regarding our shared payment integrity and efficiency goals, and setting up a plan to achieve those goals; and (2) ensuring that the Treasury DOGE Team was leveraging its unique technological expertise to help operationalize the President's policy priorities for the early days of the Administration, including by helping identify payments that may be improper under his new Executive Orders.
13. Coming out of these early conversations, on January 26, 2025, BFS initiated a 4-6 week payment process engagement plan ("engagement") in which BFS would support the Treasury DOGE Team in understanding payment processes and identifying opportunities to advance payment protection, government efficiency, and fraud reduction goals. The objective of the engagement is to gain insight into the full, end-to-end payment process across multiple BFS payment systems, and to identify data gaps that, if resolved, would make the system to work more efficiently and securely.

14. One initial goal of the engagement was to ensure that all payments through BFS's payment systems included Treasury Account Symbols (TAS) and Business Event Type Codes (BETCs), which are used to identify what type of payment and accounts each payment request is associated with. These are the kinds of enhanced controls suggested in the March 30, 2023 GAO Report. BFS has three separate primary payments systems (PAM, ASAP, ITS.gov) that support payments on behalf of nearly 250 agencies. These payment systems feed into CARS, which is a system that agencies use to track how payments should be accounted for budgetary purposes. PAM, or Payment Automation Manager, is the most widely used of BFS's payment systems. Within PAM, there are two types of payments, known as Type A and Type B—Type A is for high value, low volume payments, while Type B applies to lower value, higher volume payments. At present, a significant number of Type B payments are often missing TAS and BETC codes, meaning that payor agencies are required to modify the payment records in CARS well after payments have been certified and processed. As a result, I believe that certain of these payments cannot be accounted for accurately in CARS, and cannot be correctly connected in CARS to particular programs or purposes even after the money has been spent. The Treasury DOGE Team agreed to help address this issue as part of its preliminary work plan, in support of its goal of modernizing and identifying efficiencies.
15. Because an important part of our work was to understand the full end-to-end payment process, across multiple payment systems, this work required review of the source code for BFS's payment systems and databases across multiple BFS payment systems as well as the ability to review sensitive payment data. The Treasury Secretary, through his Chief of Staff, approved the engagement in the early days of the new Administration. Because such access

could present risks, including potential disruptions to BFS's payments systems, cybersecurity vulnerabilities, insider threat risks, and other risks that are inherent to any user access to sensitive IT systems, BFS recommended multiple mitigation measures. While these measures could not fully guarantee that the risks would not materialize, they would significantly reduce their likelihood. BFS and the DOGE Team implemented a number of mitigation measures, including physical and technical controls, instructions on proper data handling and safeguarding, and BFS staff oversight, to protect sensitive data and minimize the potential of disruptions to systems from the DOGE Team's work, as further explained in the accompanying Declaration of Joseph Gioeli.

16. The engagement remains in its initial stages—the Treasury DOGE Team was still in the process of being granted the agreed-upon levels of access to BFS databases and source code when Mr. Elez resigned. To my knowledge, as of the date of his resignation, Mr. Elez had access to and was analyzing copies of the source code for certain BFS payment systems in a secure, contained environment that was not connected to any production or test environments; thus, Mr. Elez had no ability to change BFS payments or the BFS payment system. Further, Mr. Elez had read-only access to the PAM and SPS² payment databases, subject to the agreed-upon mitigations and BFS oversight. My only access to these systems was so-called “over the shoulder” access to watch as other people were working within the systems or with data from the system. However, on February 8, 2025, an Order issued in this case restricted my access to certain BFS data and systems. I have received guidance on compliance with that Order from Treasury attorneys and am complying with that guidance.

² As noted in the Gioeli Declaration, I understand from BFS that there was briefly an error that provided Mr. Elez read/write access to the SPS system, but that Mr. Elez did not access that system during that time, and was likely unaware that he had any such read/write access.

17. As part of the Treasury DOGE Team’s efforts to assist payor agencies in identifying payments that may have been improper under the President’s Executive Orders, we received direction from Treasury leadership that the Treasury DOGE Team and BFS help agencies effectuate the President’s Executive Orders requiring pauses to certain types of financial transactions, including with respect to foreign development assistance. Specifically, under the President’s January 20, 2025 Executive Order, entitled “Reevaluating and Realigning United States Foreign Aid,” the President required that agencies pause all foreign development assistance for assessment of programmatic efficiencies and consistency with United States foreign policy. Section 3(e) of the order authorized the Secretary of State to issue waivers that would authorize specific payment programs to move forward notwithstanding the pause.
18. The Treasury DOGE Team, with assistance from BFS, was well positioned to facilitate the State Department’s review of potentially applicable payments to determine if an exemption under Section 3(e) applied. Upon direction from Treasury leadership, we worked with BFS to identify particular categories of payments potentially implicated by the Executive Order, that should be reviewed by the State Department prior to payment, consistent with the Executive Order’s requirements.
19. Specifically, the Treasury DOGE Team and BFS developed a process that would allow the State Department to review such payments prior to the payor agency’s certification of the payments for BFS processing. In the normal course, when an agency initially provides a payment file to BFS through its PAM system, BFS conducts certain reviews of that file (known as “pre-edit”) before requesting that the agency certify the payment, after which point the file is processed through BFS’s systems. An example of a check that occurs during

the pre-certification phase is to compare the payments in the file against the Do Not Pay working system, which is used to identify payments that may be improper or fraudulent. If transaction(s) in a payment file lead to a match when screened through the Do Not Pay working system, BFS notifies the submitting agency, which is given an opportunity to reexamine the payment file to determine whether to ultimately certify it for processing.

20. Our work to implement the President's foreign aid Executive Order was intended to operate similarly. The plan we implemented included identifying payments files in the pre-edit phase, prior to certification and processing, that may fall within the scope of the Executive order and, thus, require review by the State Department, as the authorized agency under the Executive Order, to determine whether they fall within the scope of the Executive Order but should receive a waiver, or whether instead the payor agency should pause the payment pursuant to the Executive Order. Starting on January 31, 2025, BFS and the Treasury DOGE Team collaborated to operationalize this process for the State Department, by identifying incoming payments that matched certain Treasury Account Symbols (TAS) associated with foreign aid payments, and flagging those payments for the State Department for review consistent with the Executive Order. BFS and the Treasury DOGE Team emphasized to the State Department that its review of identified payments should be conducted within one business day to minimize delays where payment should be authorized. At no point did BFS refrain from transmitting a payment that had been duly certified by the payor agency, because, once certified, BFS is obliged to process the payment. As described further in the Declaration of Vona S. Robinson filed concurrent with my declaration, only two sets of payments have thus far been flagged through this process; the first, on February 7, 2025, was determined by the State Department not to fall within the scope of the Executive Order.

Those payments proceeded as planned. The second, on February 10, was flagged for the State Department and later canceled by the requesting agency.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 2/11/25

Signed: 

Thomas H. Krause, Jr.
Senior Advisor for Technology and Modernization
United States Department of the Treasury

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

STATE OF NEW YORK, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF THE
TREASURY, *et al.*,

Defendants.

Civil Action No. 25-1144 (JAV)


DECLARATION OF MICHAEL J. WENZLER

Pursuant to 28 U.S.C. § 1746, I hereby declare as follows:

I, Michael J. Wenzler, declare the following to be a true and correct statement of facts:

1. I am the Associate Chief Human Capital Officer for Executive and Human Capital Services at the Departmental Offices of the Department of the Treasury (Treasury). In this capacity, I am responsible for leading and overseeing the development and delivery of the full range of human resources services to managers, supervisors, and employees of Treasury's Departmental Offices. This includes, but is not limited to, appointing, onboarding, and providing executive resources support to Departmental Offices senior executives, senior level executives, non-career executives, Schedule C appointees, and Presidential appointees. I have held this position since January 28, 2024. Prior to this role, I served at the U.S. Mint, and I have been employed at the Treasury Department since April 2020.

2. The purpose of this declaration is to set forth information related to Treasury's employment of Thomas H. Krause, Jr., and Marko Elez. The statements made herein are based

 2/11/2025

on my personal knowledge and review of documents and information furnished to me in the course of my official duties.

3. On January 23, 2025, Thomas H. Krause, Jr., was appointed under 5 U.S.C. § 3109 as a Consultant for Treasury (Departmental Offices, Office of the Chief of Staff) with the title of Senior Advisor for Technology and Modernization. Thomas executed his appointment affidavit and affirmed his oath of office on January 23, 2025 and onboarded at Treasury the same day. Consultants appointed under 5 U.S.C. § 3109 are Federal civil service employees under 5 U.S.C. § 2105. *See* 5 C.F.R. § 304.101. A consultant appointed under 5 U.S.C. § 3109 may be employed without pay. *See* 5 C.F.R. § 304.102(h). Thomas waived compensation in writing and is serving unpaid.

4. Thomas is designated as a Special Government Employee (SGE) under 18 U.S.C. § 202. An SGE is an officer or employee who is retained, designated, appointed, or employed, to perform temporary duties either on a full-time or intermittent basis, with or without compensation, for not more than 130 days during any period of 365 consecutive days.

5. On February 3, 2025, I executed human resources forms associated with Thomas's appointment ("appointment documentation") in my role as the Appointing Official. It is common during transitions between administrations, when many individuals are onboarding in a short period of time, for such appointment documentation to be executed after the individual's employment at Treasury begins. Subsequent review of the appointment documentation I executed on February 3, 2025 identified an error in the identified period of Thomas's appointment. Specifically, the February 3, 2025 documentation erroneously stated that Thomas's start date was February 9, 2025. As described above, Thomas has been a Treasury employee since January 23, 2025. Accordingly, on February 10, 2025, I executed revised appointment

MW 2/11/2025

documentation for Thomas, which reflects the correct appointment term of January 23, 2025 to March 24, 2025.

6. The Summary of Duties for Thomas's appointment states that: "The Senior Advisor will work very closely with the Office of Fiscal Assistant Secretary and Fiscal Service - and in particular the Office of the Commissioner to execute Fiscal's mission of promoting the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services. The Senior Advisor shall focus on key issues for Fiscal, including but not limited to: (1) Operational Resiliency; (2) Advancing Governmentwide Payment Integrity; (3) Critical Modernization Programs; (4) Improving the Payment Experience; and (5) TreasuryDirect User Credential Costs. The Senior Advisor shall work closely with key internal, external, and interagency stakeholders to execute Fiscal's mission."

7. 5 C.F.R. § 304.102(b) defines a consultant as "a person who can provide valuable and pertinent advice generally drawn from a high degree of broad administrative, professional, or technical knowledge or experience." 5 C.F.R. § 304.103(c) defines a consultant position as "one that requires providing advice, views, opinions, alternatives, or recommendations on a temporary and/or intermittent basis on issues, problems, or questions presented by a Federal official." Agencies may not employ consultants to preform managerial or supervisory work. *See* 5 C.F.R. § 304.103(b).

8. At the request of the Treasury Chief of Staff (hiring manager), my office is pursuing the employment of Thomas as the Senior Advisor for Technology and Modernization under a Temporary Transition Schedule C appointment (*see* 5 C.F.R. § 213.3302; [U.S. Office of Personnel Management Memorandum for Heads of Executive Departments, Independent](#)

 2/11/2025

Agencies, Inspectors General and the Council of the Inspectors General on Integrity and Efficiency dated January 8, 2025). Upon appointment, Thomas will work closely with the Chief of Staff, the Under Secretary for Domestic Finance, and the Office of Fiscal Assistant Secretary and Fiscal Service to lead the development, execution, and management of the information technology and technological modernization efforts and programs for the Department of the Treasury and the internal management of the Department and its bureaus – including the Bureau of the Fiscal Service – as it relates to technology. Mr. Krause’s new Schedule C appointment to this position has not yet occurred, but will likely occur in the near future.

9. On January 21, 2025, Treasury appointed Marko Elez as Special Advisor for Information Technology and Modernization (Treasury Departmental Offices, Office of the Chief of Staff), under Treasury’s authority to establish temporary transitional Schedule C positions. *See* 5 C.F.R. § 213.3302. Appointments under this authority may be made for a period not to exceed 120 days with one extension of an additional 120 days. As described herein, Marko was a Treasury employee between January 21 and February 6, 2025.

10. The Position Description for Marko states that his roles and responsibilities included conducting “special and confidential studies on a variety of strategies and issues related to Treasury’s information technology,” and identifying, analyzing, and making “recommendations to strengthen Treasury’s hardware and software.”

11. Although Marko could have been designated as an SGE because the appointment was to perform temporary duties either on a full-time or intermittent basis for not more than 130 days, the Treasury department Ethics office *did not* designate Marko as a Special Government Employee, meaning that Marko had to comply with additional ethics requirements that are not required for SGE positions.

 2/11/2025

12. On February 6, 2025, Marko resigned from his position. He is no longer employed by the Department of the Treasury.

See 2/11/2025

See 2/11/2025

I declare the foregoing to be true and correct, upon penalty of perjury.

Dated: 2/11/2025

Signed 

Michael J. Wenzler

Associate Chief Human Capital Officer

for Executive and Human Capital Services

Departmental Offices of the Department of the

Treasury

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STATE OF NEW YORK, *et al.*,

Plaintiffs,

- against -

DONALD J. TRUMP, IN HIS OFFICIAL
CAPACITY AS PRESIDENT OF THE
UNITED STATES, *et al.*,

Defendants.

No. 25 Civ. 1144 (JAV)

**DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO
PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION**

DANIELLE R. SASSOON
United States Attorney for the
Southern District of New York
Attorney for the United States
86 Chambers Street, Third Floor
New York, New York 10007
Tel: (212) 637-2695/2774
Attorney for Defendants

JEFFREY OESTERICHER
REBECCA S. TINIO
Assistant United States Attorneys
- Of Counsel -

TABLE OF CONTENTS

PRELIMINARY STATEMENT..... 1

BACKGROUND 1

I. The Bureau of the Fiscal Service 1

II. The United States DOGE Service..... 2

III. Review of BFS Payment Systems to Effectuate the USDS EO..... 3

IV. This Litigation..... 5

STANDARD OF REVIEW 7

ARGUMENT 7

I. Plaintiffs’ Request for Emergency Relief Violates the Separation of Powers 7

II. Plaintiffs Lack Article III Standing 10

a. Plaintiffs have not shown injury-in-fact..... 11

b. Plaintiffs have not shown causation or redressability 15

III. Plaintiffs Are not Entitled to a Preliminary Injunction 17

a. Plaintiffs fail to state an APA claim..... 18

i. Plaintiffs do not challenge final agency action 18

ii. Plaintiffs have an adequate alternative remedy 20

1. Privacy Act of 1974..... 21

2. Internal Revenue Code 23

iii. Plaintiffs have not shown a violation of any statute 25

1. Privacy Act of 1974..... 26

2. E-Government Act of 2002 28

3. Internal Revenue Code 29

4. Internal Revenue Code 29

4. Social Security Regulations..... 30

5. Title 18 Ethics Rules..... 31

- iv. Plaintiffs have not identified arbitrary or capricious agency action32
- v. Plaintiffs have not shown *ultra vires* agency action.....33
- vi. Plaintiffs have not shown a violation of the separate of powers34
- vii. Plaintiffs have not shown a violation of the Take Care Clause34
 - a. Plaintiffs have not shown irreparable harm.....35
 - b. A preliminary injunction would not serve the public interest35
 - c. The Court lacks authority to enter relief directly against the President36
- CONCLUSION36

TABLE OF AUTHORITIES

Cases

Agbanc Ltd. v. Berry,
678 F. Supp. 804 (D. Ariz. 1988) 24

Alfred L. Snapp & Son, Inc. v. Puerto Rico,
458 U.S. 592 (1982) 11

Allen v. Wright,
468 U.S. 737 (1984) 16

Amadei v. Nielsen,
348 F. Supp. 3d 145 (E.D.N.Y. 2018) 20

Apter v. Dep’t of Health & Human Servs.,
80 F.4th 579 (5th Cir. 2023) 33

Ass’n of Am. Physicians & Surgeons v. Clinton,
997 F.2d 898 (D.C. Cir. 1993)..... 9

Barclift v. Keystone Cred. Servs., LLC,
585 F. Supp. 3d 748 (E.D. Pa. 2022), *aff’d*, 93 F.4th 136 (3d Cir. 2024) 13

Bennett v. Spear,
520 U.S. 154 (1997) 19

Block v. Community Nutrition Institute,
467 U.S. 340 (1984) 20

Bohnak v. Marsh & McLennan Cos., Inc.,
79 F.4th 276 (2d Cir. 2023) 12, 14, 15

Bowen v. Massachusetts,
487 U.S. 879 (1988) 20

California v. Texas,
593 U.S. 659 (2021) 10

Cell. Assocs., Inc. v. Nat’l Insts. of Health,
579 F.2d 1155 (9th Cir. 1978) 22, 23

Citizens for Responsibility & Ethics in Washington v. Trump,
302 F. Supp. 3d 127 (D.D.C. 2018)..... 35

City of Los Angeles v. Lyons,
461 U.S. 95 (1983) 27

Clapper v. Amnesty Int’l USA,
568 U.S. 398 (1983) 10, 15, 16

Dalton v. Specter,
511 U.S. 462 (1994) 34

Dew v. United States,
192 F.3d 366 (2d Cir. 1999) 21

Doe v. Broderick,
225 F.3d 440 (4th Cir. 2000) 31

Doe v. Stephens,
851 F.2d 1457 (D.C. Cir. 1988)..... 22

Faiveley Transport Malmo AB v. Wabtec Corp.,
559 F.3d 110 (2d Cir. 2009)..... 35

Farst v. AutoZone, Inc.,
700 F. Supp. 3d 222 (M.D. Pa. 2023)..... 12

FDA v. Alliance for Hippocratic Medicine,
602 U.S. 367 (2024) 10, 14, 16

Fed. Aviation Admin. v. Cooper,
566 U.S. 284 (2012) 21, 22

Franklin v. Massachusetts,
505 U.S. 788 (1992) 36

Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.,
460 F.3d 13 (D.C. Cir. 2006)..... 18

Geyen v. Marsh,
775 F.2d 1303 (5th Cir. 1985) 33

Grand River Enter. Six Nations, Ltd. v. Pryor,
481 F.3d 60 (2d Cir. 2007) 7

Haaland v. Brackeen,
599 U.S. 255 (2023)11

Henkell v. United States,
No. 96-2228, 1998 WL 41565 (E.D. Cal. Jan. 9, 1998)..... 24

Hunstein v. Preferred Coll. & Mgmt. Servs., Inc.,
48 F.4th 1236 (11th Cir. 2022) 12

Islander E. Pipeline Co. v. McCarthy,
525 F.3d 141 (2d Cir. 2008) 33

Larson v. Domestic & Foreign Comm. Corp.,
337 U.S. 682 (1949) 33

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992) 10

Lujan v. Nat’l Wildlife Federation,
497 U.S. 871 (1990) 18

Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak,
567 U.S. 209 (2012) 25

Mississippi v. Johnson,
71 U.S. (4 Wall.) 475 (1866) 36

Moya v. U.S. Dep’t of Homeland Sec.,
975 F.3d 120 (2d Cir. 2020) 31

Murray v. Cuomo,
460 F. Supp. 3d 430 (S.D.N.Y. 2020) 11

Murthy v. Missouri,
603 U.S. 43 (2024), *remanded*, 114 F.4th 406 (5th Cir. 2024) 14

Nat’l Org. for Marriage, Inc. v. Walsh,
714 F.3d 682 (2d Cir. 2013) 34

Newdow v. Roberts,
603 F.3d 1002 (D.C. Cir. 2010) 36

Norton v. S. Utah Wilderness All.,
542 U.S. 55 (2004) 18, 19

Oklahoma v. Biden,
577 F. Supp. 3d 1245 (W.D. Okla. 2021) 36

Open Society Int’l, Inc. v. U.S. Agency for Int’l Dev.,
651 F.3d 218 (2d Cir. 2011) 13

Panjiva, Inc. v. U.S. Customs & Border Prot.,
342 F. Supp. 3d 481 (S.D.N.Y. 2018) 20

Parks v. IRS,
618 F.2d 677 (10th Cir. 1980) 22

Pearl River Union Free Sch. Dist. v. Duncan,
56 F. Supp. 3d 339 (S.D.N.Y. 2014)..... 19

Pereira v. U.S. Dep’t of Justice,
No. 16-cv-2599 (NRB), 2016 WL 2745850 (S.D.N.Y. May 11, 2016) 20

Planned Parenthood of N.Y.C., Inc. v. U.S. Dep’t of Health & Hum. Servs.,
337 F. Supp. 3d 308 (S.D.N.Y. 2018)..... 19

Poss v. Kern,
No. 23-cv-2199 (DLF), 2024 WL 4286088 (D.D.C. Sept. 25, 2024) 22

Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity,
878 F.3d 371 (D.C. Cir. 2017)..... 29

Privacy Info. Ctr. v. U.S. Dep’t of Comm.,
928 F.3d 95 (D.C. Cir. 2019)..... 29

Saget v. Trump,
375 F. Supp. 3d 280 (E.D.N.Y. 2019) 33

Salazar v. King,
822 F.3d 61 (2d Cir. 2016) 19

Seila Law LLC v. Consumer Financial Protection Bureau,
591 U.S. 197 (2020) 8, 9

Shain v. Ellison,
356 F.3d 211 (2d Cir. 2004)..... 27

Simon v. E. Ky. Welfare Rights Org.,
426 U.S. 26 (1976) 16, 17

Sprint Commc’ns Co. v. APCC Servs, Inc.,
554 U.S. 269 (2008) 16

Starbucks Corp. v. McKinney,
602 U.S. 339 (2024) 36

Students for Fair Admissions v. U.S. Mil. Acad. at West Point,
709 F. Supp. 3d 118 (S.D.N.Y. 2024)..... 7

Sussman v. U.S. Marshal Serv.,
494 F.3d 1106 (D.C. Cir. 2007)..... 22

TransUnion v. Ramirez,
594 U.S. 413 (2021) passim

Tripp v. Dep’t of Defense,
193 F. Supp. 2d 229 (D.D.C. 2002)..... 22

Trudeau v. FTC,
456 F.3d 178 (D.C. Cir. 2006)..... 28, 29

U.S. Army Corps of Eng’rs v. Hawkes Co., Inc.,
578 U.S. 590 (2016) 19

U.S. Navy SEALs 1-26 v. Biden,
578 F. Supp. 3d 822 (N.D. Tex. 2022) 36

Warth v. Seldin,
422 U.S. 490 (1975)11

Weinberger v. Romero-Barcelo,
456 U.S. 305 (1982) 36

Westcott v. McHugh,
39 F. Supp. 3d 21 (D.D.C. 2014)..... 22

Statutes

5 U.S.C. § 552a(a)(2) 21

5 U.S.C. § 552a(a)(4) 26

5 U.S.C. § 552a(b)(1)..... 26, 27, 28

5 U.S.C. § 552a(b)(4)..... 28

5 U.S.C. § 552a(e)(4) 27

5 U.S.C. § 552a(g)(1)(A) 21, 22

5 U.S.C. §552a(g)(1)(B) 21

5 U.S.C. §552a(g)(1)(D) 21

5 U.S.C. § 702..... 24

5 U.S.C. § 704..... 20

5 U.S.C. § 2103..... 27

5 U.S.C. § 3161..... 3, 4

18 U.S.C. § 202..... 25

18 U.S.C. § 202(a)	27
18 U.S.C. § 208.....	31, 32
18 U.S.C. § 208(a)	32
26 U.S.C. § 6103.....	23, 24, 29
26 U.S.C. § 6103(a)	29, 30
26 U.S.C. § 7213(a)(1).....	24
26 U.S.C. § 7431.....	24
26 U.S.C. § 7431(a)(1).....	24
31 U.S.C. § 3325(a)	17
31 U.S.C. 3365(a)	15
44 U.S.C. § 3501.....	28
Pub. L. No. 107-347.....	28
<i>Regulations</i>	
5 C.F.R. § 213.3301	27
20 C.F.R. § 422.104(a).....	31
31 C.F.R. § 1.32	31
31 C.F.R. § 1.32(d).....	30

PRELIMINARY STATEMENT

Plaintiffs bring this unprecedented and unsupported challenge to the Executive Branch's ability to exercise politically accountable oversight of agency activities and to implement the President's policy priorities. Dissatisfied with those priorities, Plaintiffs seek an emergency injunction barring duly appointed Treasury Department officials, whose responsibilities include liaising with the United States DOGE Service ("USDS"), from accessing systems in the Bureau of the Fiscal Service ("BFS" or "Bureau") necessary to perform their Presidentially-directed mandate of maximizing efficiency and productivity, including ensuring data and payment integrity with respect to the 1.2 billion transactions and over \$5 trillion in outlays handled by BFS. As demonstrated below, Plaintiffs are not entitled to the injunction they seek, which would violate the separation of powers by impermissibly intruding into the Executive's decisionmaking with respect to which Treasury Department employees are granted access to BFS systems and data, in order to provide oversight of the Department and to implement the Executive's priorities. Further, Plaintiffs lack standing, and their claims fail on the merits. The Privacy Act, underpinning the majority of Plaintiffs' claims, is only available to individuals, not governmental units. Nor can Plaintiffs rely on the Administrative Procedure Act to circumvent the Privacy Act's express restrictions. For similar reasons, Plaintiffs claims under the Internal Revenue Code and the Ethics in Government Act also fail. Accordingly, Plaintiffs' motion for a preliminary injunction should be denied.

BACKGROUND

I. The Bureau of the Fiscal Service

The Bureau of the Fiscal Service is a component of the Department of the Treasury, established in October 2012 by then-Secretary of the Treasury Timothy Geithner which

consolidated two previously separate bureaus. *Treasury Order Establishing the Bureau of the Fiscal Service*, 78 Fed. Reg. 31,629 (May 24, 2013) (Treasury Order 136-01). The Secretary's order combined the former Bureau of the Public Debt and the Financial Management Service into the BFS and established the role of BFS Commissioner to execute the functions for which the heads of those bureaus were previously responsible. *Id.*

Among other responsibilities, the Bureau is responsible for “manag[ing] the government’s accounting, central payment systems, and public debt, and . . . serv[ing] as the central payment clearinghouse for most payments to and from federal agencies.” Declaration of Thomas H. Krause, Jr., dated February 11, 2025 (“Krause Decl.”) ¶ 5. BFS’s payment systems include, among others, the Payment Automation Manager (“PAM”) System, which is the federal government’s largest system for receiving payment files and processing payments, the Secure Payment System (“SPS”), a system through which paying agencies securely create, certify, and submit payment files to Treasury, the Automated Standard Application for Payments (“ASAP”), a recipient-initiated electronic payment and information system, and the Central Accounting and Reporting System (“CARS”), which federal agencies use to account for their spending. Declaration of Joseph Gioeli III, dated February 11, 2025 (“Gioeli Decl.”) ¶¶ 6-11.

II. The United States DOGE Service

On January 20, 2025, President Trump signed Executive Order 14,158, which directs changes to the previously established United States Digital Service designed to implement the President’s agenda of “improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems.” 90 Fed. Reg. 8441, § 4 (“USDS EO”). The USDS EO also redesignated the United States Digital Service as the Department of Governmental Efficiency Service, or U.S. DOGE Service. *Id.* § 3(a). Similarly, it established a

“U.S. DOGE Service Temporary Organization” within the Executive Office of the President pursuant to 5 U.S.C. § 3161, which will terminate on July 4, 2026. USDS EO § 3(b). Agency heads are required under the USDS EO to establish within their respective agencies a DOGE Team of at least four employees, which may include Special Government Employees. *Id.* § 3(c).

The USDS EO directs USDS to collaborate with Executive agencies to modernize the technology and software infrastructure of the federal government to increase efficiency and productivity as well as ensure data integrity. *Id.* § 4. With respect to the Department of the Treasury, the need to modernize and ensure data integrity is uniquely critical: the Government Accountability Office (“GAO”) has identified “problems in accounting for transactions between federal agencies,” resulting in potentially improper payments totaling approximately \$2.7 trillion dollars. *See* GAO Report, “Financial Statement Audit: Bureau of the Fiscal Service’s FY22 Schedules of the General Fund” (March 30, 2023), *available at* [Financial Audit: Bureau of the Fiscal Service's FY 2022 Schedules of the General Fund | U.S. GAO](#) (last visited Feb. 11, 2025). Similarly, GAO has identified areas for improvement in BFS’s systems related to identifying and tracing transactions to determine whether they were complete and properly recorded in the correct general ledger accounts and line items within the Schedules of the General Fund. *Id.* In particular, GAO has found inconsistent reporting, lack of traceability, and need for improved controls within CARS. *Id.*

To accomplish its objectives, the USDS EO directs USDS to work with relevant agency heads and vice versa, to ensure USDS has access to “unclassified agency records, software systems, and IT systems” to the “extent consistent with law.” *Id.* § 4(b). At all times, the USDS EO instructs, USDS must “adhere to rigorous data protection standards.” *Id.*

III. Review of BFS Payment Systems to Effectuate the USDS EO

Thomas Krause is an employee of the Treasury Department and is the DOGE Team lead at the agency (“Treasury DOGE Team”). Krause Decl. ¶ 2. His position at Treasury as Senior Advisor for Technology and Modernization was created to effectuate the mission of DOGE by reducing and eliminating improper and fraudulent payments, addressing the problems of waste, fraud, and abuse, and improving the accuracy of financial reporting. *Id.* Currently, Mr. Krause is the only Treasury DOGE Team member. *Id.* ¶ 3. Although Mr. Krause coordinates with officials at USDS and provides them with regular updates on the team’s progress, he is not an employee of USDS. *Id.* ¶ 4. Instead, he is an employee of Treasury. Declaration of Michael J. Wenzler, dated February 11, 2025 (“Wenzler Decl.”) ¶ 5.

Mr. Krause’s role on the Treasury DOGE Team is to find ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of the current Administration. *Id.* As part of the President’s DOGE efforts, Mr. Krause’s mandate is to understand how BFS’s end-to-end payment systems and financial reporting tools work, recommend ways to update and modernize those systems to better identify improper and fraudulent payments, and better allow federal agencies to quickly adapt to changing conditions. *Id.* ¶ 10.

Mr. Krause has never had any direct access to any BFS payment system. His only access to those systems was so-called “over the shoulder” access to review activity others performed in the system or data others accessed from the system. *Id.* ¶ 16. However, under the terms of the temporary restraining order in place in this litigation, Mr. Krause does not currently have any access to BFS systems. *Id.*

A second Treasury DOGE team member, Marko Elez, began working at the Treasury Department on January 21, 2025, but resigned from his role on February 6, 2025. *Id.* ¶ 3; Wenzler

Decl. ¶ 9. Treasury hired Mr. Elez as a Special Advisor for Information Technology and Modernization. *Id.* In this role, Mr. Elez was a Treasury employee tasked with working closely with engineers at BFS on information technology matters in service of BFS’s mission to promote financial integrity and operational efficiency of the federal government through accounting, financing, collection, payment, and other relevant BFS services. *Id.* In the course of his work and subject to close supervision and a number of cybersecurity measures, Mr. Elez was provided with copies of certain BFS information and source code with which to work in a secure environment on his BFS-provided devices. Gioeli Decl. ¶¶ 11-21. Mr. Elez never “wrote” code directly to (or otherwise directly altered) any BFS systems, nor does BFS have any reason to believe that Mr. Elez transmitted any BFS data or other information outside the federal government. *Id.* On February 6, 2025, Mr. Elez submitted his resignation from this role. *Id.* ¶ 22. On that same day, he turned in his government-issued laptops, access card, and other government devices; his BFS systems access was terminated; and he has not conducted any work related to the BFS payment systems since that date. *Id.*

IV. This Litigation

On February 7, 2025, plaintiff State of New York, together with eighteen additional states, filed a Complaint for Declaratory and Injunctive Relief in this matter against Donald J. Trump, in his official capacity as President of the United States, the United States Department of the Treasury, and Scott Bessent, in his official capacity as Secretary of the Treasury (collectively, “Defendants”). ECF No. 7. Plaintiffs seek, *inter alia*, a temporary restraining order and permanent injunction barring Defendants from (i) granting to political appointees, special government employees, and any government employee detailed from an agency outside the Treasury Department access to any Treasury Department payment or data systems containing personally identifiable information

and/or confidential financial information of payees, and ordering any such person who has unlawfully received such information to destroy or return it; (ii) granting access to Treasury Department payments or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees to any person unless that person has passed all background checks, security clearance, and mandated information security training, and otherwise excluding political appointees and special government employees; and (iii) declaring that granting access to political appointees, special government employees, and any government employee detailed from an agency outside the Treasury Department to any Treasury Department payment or data systems containing personally identifiable information and/or confidential financial information of payees is agency action that is ultra vires, unlawful, and unconstitutional. *Id.* at 55. Plaintiffs allege in their Complaint that the Treasury Department changed its policy regarding access to its payment and data systems in violation of the Administrative Procedure Act (“APA”) and other statutes and that the alleged new policy violates the Separation of Powers and Take Care Clause of the Constitution. *Id.* at 46-55.

On Saturday, February 8, without hearing from Defendants, the District Judge sitting in Part I entered a Temporary Restraining Order that largely adopted the proposed order offered by Plaintiffs. In relevant part, the Court’s Ex Parte Order (ECF No. 6) provides that Defendants are:

(i) restrained from granting access to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees, other than to civil servants with a need for access to perform their job duties within the Bureau of Fiscal Services who have passed all background checks and security clearances and taken all information security training called for in federal statutes and Treasury Department regulations; (ii) restrained from granting access to all political appointees, special government employees, and government employees detailed from an agency outside the Treasury Department, to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial

information of payees; and (iii) ordered to direct any person prohibited above from having access to such information, records and systems but who has had access to such information, records, and systems since January 20, 2025, to immediately destroy any and all copies of material downloaded from the Treasury Department's records and systems, if any.

On February 9, 2025, Defendants filed an Emergency Motion to Dissolve, Clarify, or Modify the Ex Parte Temporary Restraining Order. (ECF No. 11). On February 11, 2025, the Court granted in part and denied in part Defendants' motion. (ECF No. 28).

STANDARD OF REVIEW

“A preliminary injunction ‘is an extraordinary and drastic remedy, one that should not be granted unless the movant, by a clear showing, carries the burden of persuasion.’” *Students for Fair Admissions v. U.S. Mil. Acad. at West Point*, 709 F. Supp. 3d 118, 129 (S.D.N.Y. 2024) (quoting *Grand River Enter. Six Nations, Ltd. v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007)). To obtain a preliminary injunction, the movant must establish “(1) irreparable harm absent injunctive relief; (2) a likelihood of success on the merits; and (3) that a preliminary injunction is in the public interest.” *Id.* (citations and footnote omitted).

ARGUMENT

Plaintiffs are not entitled to relief because the extraordinary injunction they seek would violate the separation of powers. Plaintiffs' proposed order creates an arbitrary distinction between classes of Executive Branch employees and intolerably inhibits the President's exercise of his constitutional functions.

Even were this not the case, Plaintiffs' suit suffers from a different foundational defect: they lack standing to bring it. In addition, Plaintiffs do not, and cannot, meet the threshold requirements for alleging an APA claim as they have not identified final agency action, and thus have no cause of action. Moreover, Plaintiffs have failed to establish a likelihood of success on

the merits, failed to identify irreparable harm, and failed to show that the balance of the equities favors them. Their motion therefore should be denied.

I. Plaintiffs' Request for Emergency Relief Violates the Separation of Powers

Plaintiffs' motion seeks relief that is constitutionally infirm. Without any precedent, Plaintiffs seek to limit access to Treasury systems and records to only "civil servants"—a term that is undefined in the Complaint—while prohibiting "all political appointees, special government employees, and government employees detailed from an agency outside the Treasury Department" from access to such systems and records, regardless of their need for such information in the performance of their duties, including duties specifically tasked to them by the President. *See* ECF No. 7 at 55.

This distinction between "civil servants" and all other types of government officials is not grounded in any statute passed by Congress and signed by the President. Plaintiffs have cited no statute supporting such a distinction between "career" officials and all other Executive Branch employees, and the distinction is entirely illusory. Both "career" and political employees of the Executive Branch serve the President and are charged with advancing his priorities. Any suggestion otherwise conflicts with basic separation of powers principles that dictate that the President's access to information and ability to seek advice and give direction to his subordinates – whether career or non-career – is necessary to Article II. This Court should reject Plaintiff's unbriefed and unsupportable invitation to reach such a result.

"Under our Constitution, the 'executive power'—all of it—is vested in a President," who must "take Care that the laws be faithfully executed." *Seila Law LLC v. Consumer Financial Protection Bureau*, 591 U.S. 197, 203 (2020) (quoting U.S. CONST. art. II, § 1, cl. 1; *id.*, § 3). "Because no single person could fulfill that responsibility alone, the Framers expected that the

President would rely on subordinate officers for assistance.” *Id.* at 203-04. To that end the President may, for example, “require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Offices.” *Id.* § 2, cl. 1; *see also Ass’n of Am. Physicians & Surgeons v. Clinton*, 997 F.2d 898, 909 (D.C. Cir. 1993) (“Article II not only gives the President the ability to consult with his advisers confidentially, but also, as a corollary, it gives him the flexibility to organize his advisers and seek advice from them as he wishes.”).

In order to give meaningful advice, the President’s subordinates, including and especially his closest advisors, who are generally political appointees, must be able to gather the information necessary to render that advice useful and accurate. Walling those subordinates off from critical sources of information hinders their ability to offer—and for the President to receive—advice the Constitution specifically requires them to provide. And restricting “special government employees and government employees detailed from an agency” compounds the problem, by further restricting the pool of individuals from whom the President and his direct appointees can receive meaningful advice, regardless of those individuals’ skills, expertise, or need for information.

Likewise, the restrictions Plaintiffs seek run afoul of the Constitution because they limit the President’s ability to give direction to his subordinates. As the Supreme Court has emphasized, under the “constitutional strategy” chosen by the Framers, “individual executive officials will still wield significant authority, but that authority remains subject to the ongoing supervision and control of the elected President.” *Seila*, 591 U.S. at 224. If executive officers are categorically walled off from entire sources of information, they cannot provide the President with full information and the President in turn cannot properly supervise and direct his subordinates .

Tellingly, Plaintiffs have cited no statute supporting a distinction between “career” officials and all other Executive Branch employees for this purpose. That is because this distinction conflicts with basic separation of powers principles. This Court therefore should deny Plaintiffs’ request for a preliminary injunction as unconstitutional.

II. Plaintiffs Lack Article III Standing

The Court should deny the preliminary injunction for the additional reason that Plaintiffs lack standing. A mandatory prerequisite to any exercise of judicial power under Article III, including the provision of emergency relief, is the existence of a constitutional “case” or “controversy,” without which the Court lacks jurisdiction to proceed. *FDA v. Alliance for Hippocratic Medicine*, 602 U.S. 367, 378 (2024); *see also id.* at 381 (“By requiring the plaintiff to show an injury in fact, Article III standing screens out plaintiffs who might have only a general legal, moral, ideological, or policy objection to a particular government action.”).

Establishing standing requires three showings. The plaintiff must show a “concrete” (“real,” not “abstract”) injury-in-fact, which is “particularized” to the plaintiff and not a “generalized grievance.” *Alliance*, 602 U.S. at 381. If the injury has not yet actually manifested, it must be “certainly impending,” and not speculative. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (1983). And even an alleged actual—*i.e.*, present—injury must be legally cognizable under the American legal tradition. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424-26 (2021). If a plaintiff can show injury-in-fact, she must also show the second element: a causal link between that injury and the allegedly unlawful conduct of the defendant. *Alliance*, 602 U.S. at 382. In the context of a challenge to governmental action that does not directly impact the challenger, causation will be “ordinarily substantially more difficult to establish,” *id.* (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 562 (1992) (internal quotation marks omitted)), because the plaintiff

“generally cannot ‘rely on speculation about the unfettered choices made by independent actors not before the courts,’” *id.* at 383 (quoting *Clapper*, 568 U.S. at 415 n.5). Finally, the plaintiff must show that any injury caused by the allegedly unlawful behavior of the defendant is likely redressable by judicial relief. *California v. Texas*, 593 U.S. 659, 671-74 (2021).

Because the Plaintiff States have not shown any of the three foundational requirements of standing, the Court cannot reach the merits of their motion, which therefore must be denied. *Murray v. Cuomo*, 460 F. Supp. 3d 430, 438 (S.D.N.Y. 2020).

a. Plaintiffs have not shown injury-in-fact.

The Plaintiff States fail to establish injury-in fact. The States allege only one form of present, concrete injury: that a purportedly unauthorized, “expanded group of people at Treasury” now has access to “*their* sensitive bank information and other sensitive financial data” stored on BFS systems. ECF No. 4 at 11 (emphasis added). Importantly, Plaintiffs limit their allegations of injury to *their own* information; they correctly do not make a *parens patriae* argument on behalf of their citizens or residents, which would be unavailable to them in any event. *Haaland v. Brackeen*, 599 U.S. 255, 294-95 (2023) (citing *Alfred L. Snapp & Son, Inc. v. Puerto Rico*, 458 U.S. 592, 610 n.16 (1982)).

To be clear, there has been no “unauthorized” access. *See infra*. But even assuming (solely for purposes of Defendants’ opposition, *see, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975)), that there had been such unauthorized access, Plaintiffs still fail to establish standing.

Unauthorized access alone would not give rise to an actual, concrete harm sufficient to establish standing. *TransUnion*, 594 U.S. at 426-27, leaves no doubt that a statutory violation is not, by itself, a cognizable constitutional injury. Rather, “[o]nly those plaintiffs who have been

concretely harmed by a defendant’s statutory violation may sue that . . . defendant over that violation in federal court.” *Id.* at 427 (emphasis in original).

Plaintiffs appear to suggest, incorrectly, that “unauthorized” disclosure alone is a basis for standing, apart from a separate risk of injury emerging from that purported disclosure. ECF No. 4 at 12-13. Plaintiffs nevertheless insist that they have been actually harmed, analogizing the access at issue here to the “intangible harm arising from disclosure of one’s [personally identifiable information]” that the Second Circuit deemed sufficient for standing in *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 286 (2d Cir. 2023). ECF No. 4 at 12-13. This claim, assuming it is actually being pressed, cannot establish their standing.

To start, *Bohnak* is distinguishable. In *TransUnion*, the Supreme Court observed that some “intangible harms” may qualify as injury in fact, particularly when those harms have a “close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts.” 594 U.S. at 425; *see also id.* at 424 (the concreteness “inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury”). The Court made clear, however, that this inquiry “is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts.” *Id.* at 424-25. *Bohnak* applied that logic and found that the disclosure of the plaintiff’s personal information “to an unauthorized malevolent actor,” 79 F.4th at 286, bore a close relationship to the traditional tort of “disclosure of private information,” *id.*

The logic of *Bohnak* does not apply here. Even assuming that a State can have “personal information” comparable to a natural person—a proposition that Plaintiffs never establish—that the claim at issue requires *public* disclosure. *See Hunstein v. Preferred Coll. & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240, 1245-50 (11th Cir. 2022) (en banc) (no cognizable injury from disclosure of

private information where plaintiff's information was sent from hospital to collection agency because disclosure was not public); *id.* at 1246 (citing cases); *Farst v. AutoZone, Inc.*, 700 F. Supp. 3d 222, 231-32 (M.D. Pa. 2023) (discussing the tort and distinguishing *Bohnak*); Rest. 2d of Torts § 652D ("Publicity given to private life"); *see also TransUnion*, 594 U.S. at 434 n.6 ("Many American courts did not traditionally recognize intra-company disclosures as actionable publications for purposes of the tort of defamation." (citations omitted). Even taking Plaintiffs' allegations as true, it is clear that there has been no public disclosure here; instead, there has been (at most) an exchange internal to the federal government. *Barclift v. Keystone Cred. Servs., LLC*, 585 F. Supp. 3d 748, 758-59 (E.D. Pa. 2022) ("Even assuming that the employees of the mailing vendor read Barclift's personal information, sharing her personal information with 'a small group of persons is not publicity.'" (citation omitted)), *aff'd*, 93 F.4th 136, 146 (3d Cir. 2024) ("Like our sister circuits, we conclude that the harm from disclosures that remain functionally internal are not closely related to those stemming from public ones."). Plaintiffs do not allege—much less establish—that the employees with access to the BFS systems have disclosed any information to unauthorized persons, let alone in a way that caused tangible harm. There is thus no cognizable injury from the employees' access, authorized or not.

Plaintiffs also claim harm in the form of an infringement of their "reasonable expectation that their sensitive financial information" would be "securely held in accordance with governing law and basic cybersecurity principles." ECF No. 4 at 12. However, the complaint and motion are devoid of any plausible allegation that the access of which Plaintiffs complain materially compromises the security of their data, including as measured against relevant cybersecurity principles. This claim, then, amounts to an allegation that Plaintiffs expected their personal information to be handled a certain way, and it was not. Plaintiffs cite no authority for this standing

theory of harm to reasonable expectations, or facts supporting that such handling requirements were, in fact, a reasonable expectation, as they have the burden to do. *All. for Open Society Int'l, Inc. v. U.S. Agency for Int'l Dev.*, 651 F.3d 218, 227 (2d Cir. 2011) (“Plaintiffs bear the burden of establishing standing.”). The absence of on-point authority is perhaps unsurprising: were it enough for a plaintiff to establish standing simply by alleging that the holder of personal information used it in a manner contrary to the plaintiff’s subjective expectations, the limits the Supreme Court and Second Circuit have carefully established to govern when disclosure of information constitutes injury-in-fact, including the requirement to identify a historical analogue, would be eliminated. *See generally TransUnion*, 594 U.S. at 424-25; *Bohnak*, 79 F.4th at 286.

Plaintiffs also allege a “substantial risk” of future harms stemming from the access they claim is unlawful, but their conjecture is too speculative and attenuated to support standing. First, Plaintiffs claim that access to information will lead to an “increased risk of interference, fraud, and unauthorized access,” ECF No. 4 at 12, by which they appear to mean that the expanded “access significantly heightens the risk that the BFS payment systems—and the States that interact with them—will be far more vulnerable to hacking or activities that render the information corrupted or compromised.” *Id.* at 13. Plaintiffs do not argue that the DOGE individuals themselves will “hack” the information, but that their actions will make the underlying information more vulnerable to third-party hackers. *Id.* This speculative supposition is directly contradicted by the declarations in the record regarding the extensive security mitigation measures Treasury has employed, *see* Gioeli Decl. ¶¶ 11-15; Krause Decl. ¶ 15, and not a basis for standing. For Plaintiffs’ theory to be correct, they would have to demonstrate: (1) that access by the DOGE individuals will materially increase the risk of hacking, notwithstanding Treasury’s existing internal controls and extensive mitigation efforts (*see* Gioeli Decl. ¶¶ 11-15; Krause Decl. ¶ 15); (2) that there will be a

cybersecurity incident that will compromise Treasury’s information; (3) that the States’ information specifically will be compromised; and (4) that compromise will cause the States’ cognizable harm. This “chain of causation is simply too attenuated.” *Alliance*, 602 U.S. at 392; *Murthy v. Missouri*, 603 U.S. 43, 57 (2024) (“The one-step-removed, anticipatory nature of [plaintiffs’] alleged injuries” fails to satisfy standing), *remanded*, 114 F.4th 406 (5th Cir. 2024); *Clapper*, 568 at 416.

In this respect, Plaintiffs’ allegations are again unlike *Bohnak*. In *Bohnak*, unlike here, there *had* been a breach of the plaintiff’s information outside of the defendant entity and the plaintiff *had* incurred expenses in response to that breach which the court had determined to be cognizable. *See* 79 F.4th at 285-86. Here, both disclosure and response are entirely speculative and indeed rebutted by the factual record.

Plaintiffs’ second ground for claiming standing also fails. The States’ allegation that “allowing access to this information enables those with newly-gained access to block or impede critical funding payments to States under their federal grants—which they have recently expressed as their prime objective,” ECF No. 4. at 13, is also insufficient to establish injury-in-fact. Plaintiffs would have to identify not only that their funding was reduced, but also that the Treasury DOGE Team’s access was the but-for cause of that reduction. However, Treasury cannot legally disburse a payment that has not been certified by the payor agency, nor does it have the discretion to refuse (and has not in fact refused) to disburse any certified payment. *See* 31 U.S.C. § 3365(a); Declaration of Vona S. Robinson, dated February 11, 2025 (“Robinson Decl.”) ¶ 5. Ultimately, if a payor agency refused to certify payments that Plaintiff States believe were legally owed, they would be free to bring a suit against those payor agencies. But such a threat must be “certainly impending” first; Plaintiffs lack standing to seek such relief here. *Id.* at 416..

Indeed, this allegation is telling. Plaintiffs' real complaint appears to be that through the work of DOGE, some of their funds may be blocked in the future. That suggestion is too speculative on this record to establish standing. *See Clapper* 568 U.S. at 411, 416.

b. Plaintiffs have not shown causation or redressability.

Plaintiffs also cannot establish causation or redressability. As discussed *supra*, the only direct injuries Plaintiffs have alleged from the purportedly unlawful access at issue are disclosures to unauthorized individuals and impingement on expectations. ECF No. 4 at 11-12. For the reasons given above, those purported harms are not legally cognizable.

The remaining injuries Plaintiffs have hypothesized—data security vulnerabilities and loss of funding—are so attenuated that they not only fail to qualify as injuries-in-fact, *see supra*, but also have an insufficient causal relationship with the “allegedly unlawful conduct” of Defendants, *i.e.*, the granting of access to certain Treasury systems for certain purposes. *See Allen v. Wright*, 468 U.S. 737, 751 (1984). For analogous reasons, these injuries, even if the Court accepts them as sufficiently substantiated, are not remediable by a judicial order. *See Alliance*, 602 U.S. at 380-81 (“The second and third standing requirements—causation and redressability—are often ‘flip sides of the same coin.’” (quoting *Sprint Commc’ns Co. v. APCC Servs, Inc.*, 554 U.S. 269, 288 (2008))).

The first future injury Plaintiffs identify is “the risk that the BFS payment systems—and the States that interact with them—will be far more vulnerable to hacking or activities that render the information corrupted or compromised.” As detailed above, to deem this injury constitutionally adequate requires accepting a conjectural chain of future events. *See supra*. Not only does each step in this chain make the injury complained-of itself less likely to occur, but it stretches beyond legal cognizability any connection between the conduct alleged to be unlawful

(the agency’s provision of access to the BFS systems) and the feared consequence (exploitation of data). This “speculative chain of possibilities” bears a close resemblance, in this respect, to the allegations the Supreme Court rejected as insufficient for both injury-in-fact and causation in *Clapper*. 568 U.S. at 410-14. In particular, accepting Plaintiffs’ theory entails endorsing a “standing theor[y] that rest[s] on speculation about the decisions of independent actors”—here, malicious actors online who would obtain and exploit Plaintiffs’ data. *Id.* at 414; *see also Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 42-43 (1976). Redressability is also absent here, because a court order denying access to an undefined set of “political appointees” or other employees Plaintiffs apparently wish to exclude would not meaningfully affect the likelihood of a future cyber intrusion incident that could lead to the same harms Plaintiffs identify. *See Simon*, 426 U.S. at 45-46; *see also* Gioeli Decl. ¶¶ 11-15 (describing mitigation measures).

The potential that Plaintiffs will lose federal funding in the future is equally causally attenuated and unlikely to be redressed by success in this litigation. *See* ECF No. 4 at 13. To substantiate their concern, Plaintiffs point to statements made by the President and Elon Musk expressing a desire to limit or eliminate wasteful or inappropriate government expenditures. *Id.* (citing Compl. ¶¶ 136, 141, 174). Regardless of Plaintiffs’ objections to the President’s policy objectives, it strains credulity to claim that *if* the spending reductions discussed come to pass, and *if* they affect Plaintiffs, that policy is the result of the BFS access Plaintiffs have sued to enjoin.

Furthermore, redressability is lacking because Plaintiffs fail to establish that absent the access by the Treasury DOGE Team that they seek to enjoin, the feared reduction in federal funding would not occur. Treasury has no authority to make payments that have not been certified by payor agencies, and no discretion to make payments that the paying agency has certified. 31 U.S.C. § 3325(a). This again highlights the fact that Plaintiffs’ real grievance here is with policy choices,

not access to BFS systems. If a payor agency has refused or failed to certify a payment, Treasury cannot legally disburse it, no matter who does or does not have access to BFS systems.

III. Plaintiffs Are not Entitled to a Preliminary Injunction.

Beyond the constitutional infirmity of the relief they are requesting and Plaintiffs' lack of standing, Plaintiffs' request for a preliminary injunction fails also because they cannot establish a likelihood of success on the merits of their APA or constitutional claims.

a. Plaintiffs fail to state an APA claim.

i. Plaintiffs do not challenge final agency action.

Plaintiffs' three claims under the APA, Compl. ¶¶ 154-99, fail to satisfy several threshold prerequisites. As an initial matter, the law is clear that the APA does not permit "judicial review over everything done by an administrative agency." *Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 19 (D.C. Cir. 2006) (quotation omitted). Rather, APA review is limited to "final agency action." *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 61-62 (2004) (quoting 5 U.S.C. § 704) ("SUWA").

Plaintiffs attempt to meet that requirement by asserting that Treasury previously had a policy restricting access to its BFS systems to "career civil servants with a need for access" the systems, a policy that was purportedly changed to allow "Special Government Employees ("SGEs") to access the systems. ECF No. 4 at 10. But Plaintiffs point to no written rules, orders, or even guidance documents that set forth the supposed prior access policy, or the challenged "change" to that policy. Instead, Plaintiffs appear to have attached a "policy" label to their own amorphous description of Treasury's practices. But a final agency action requires more. *See Lujan v. Nat'l Wildlife Federation*, 497 U.S. 871, 890 (1990) (rejecting challenge to Bureau of Land Management's so-called "land withdrawal review program"—a program that was not derived from

any authoritative text, but was instead the agency’s own term for describing certain continuing operations).

Moreover, even assuming *arguendo* this policy both existed and was changed—neither of which is true, *see* Gioeli Decl. ¶ 23—Plaintiffs have not established that the so-called “access policy,” *id.* at 11, constitutes final agency action. That is because agency action is final only when it “mark[s] the consummation of the agency’s decisionmaking process” and is “one by which rights or obligations have been determined, or from which legal consequences will flow.” *U.S. Army Corps of Eng’rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997)).

Here, final agency action is absent on the basis of the second prong alone. *See Pearl River Union Free Sch. Dist. v. Duncan*, 56 F. Supp. 3d 339, 366 (S.D.N.Y. 2014). Even before the entry of the TRO, Mr. Krause did not have direct access to any Treasury systems, and Mr. Elez (before his resignation) was provided with limited access as necessary to perform his duties as a Treasury employee. He was able to view and work with copies of code and some data from the BFS systems in assisting the Department to exercise its lawful functions. Krause Decl. ¶ 15; Gioeli Dec. ¶¶ 11-21. This is the type of day-to-day operation of governmental programs that does not fall into APA review. *See SUWA*, 542 U.S. at 63-64.

Even if the Treasury DOGE Team’s access to BFS systems was final vis-à-vis the agency, it creates no immediate legal effects for Plaintiffs, and so is not final with respect to them. *See Planned Parenthood of N.Y.C., Inc. v. U.S. Dep’t of Health & Hum. Servs.*, 337 F. Supp. 3d 308, 328 (S.D.N.Y. 2018) (“For [the second] prong, ‘the core question is whether the result of [the agency’s decisionmaking] process is one that will directly affect the parties.’” (first alteration added, second alteration in original) (quoting *Salazar v. King*, 822 F.3d 61, 82 (2d Cir. 2016))).

An allegation that unauthorized individuals accessed Plaintiffs' data does not establish finality on the second prong. To establish finality, Plaintiffs would need to show that their data has, in fact, been improperly disclosed (including to the Treasury DOGE Team)—not just that the Team had access to it. By analogy, an agency's decision to give an employee a work computer is not itself final agency action, even if the employee might conceivably use the computer to effect final agency action (*e.g.*, in approving or denying benefits).

Plaintiffs' cited authorities do not compel a contrary conclusion. It may be that "a plaintiff can satisfy the finality requirement without offering evidence of a formal or official statement regarding the agency's position," ECF No. 4 at 16 (quoting *Amadei v. Nielsen*, 348 F. Supp. 3d 145, 165 (E.D.N.Y. 2018)), but the requirements of finality—that the agency has consummated its decisionmaking process, and that the decision determined legal rights and obligations—apply in the context of any alleged final agency action, formal or not. Those requirements are not met here.

ii. Plaintiffs have an adequate alternative remedy.

Plaintiffs' APA causes of action fail for the additional, independent reason that the statute does not apply where there is "[an]other adequate remedy in any court." 5 U.S.C. § 704. This statutory provision "makes it clear that Congress did not intend the general grant of review in the APA to duplicate existing procedures for review of agency action." *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988). Accordingly, "[w]hen another statutory vehicle provides an adequate remedy in a court, claims brought under the APA are properly dismissed." *Panjiva, Inc. v. U.S. Customs & Border Prot.*, 342 F. Supp. 3d 481, 494 (S.D.N.Y. 2018) (quoting *Pereira v. U.S. Dep't of Justice*, No. 16-cv-2599 (NRB), 2016 WL 2745850, at *13 (S.D.N.Y. May 11, 2016)). Stated differently, where an agency action is subject to review in some manner under a statutory review scheme, then the general rule is that action must be reviewed within the confines of that scheme. In

other words, the mode of review established by the statutory review scheme is presumed exclusive. This is true even where a statutory review scheme only provides for review of issues by certain parties; other parties are presumptively precluded from obtaining review of those issues under the APA. *Block v. Community Nutrition Institute*, 467 U.S. 340, 349 (1984) (“[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded.”); *see also Dew v. United States*, 192 F.3d 366, 372 (2d Cir. 1999).

Under these principles, Plaintiffs are not entitled to challenge purported violations of the Privacy Act and the Internal Revenue Code under the APA, because each statute provides an adequate alternative remedy for persons entitled to sue under those statutes.

1. Privacy Act of 1974

The Privacy Act establishes “a comprehensive and detailed set of requirements” for federal agencies that maintain systems of records containing individuals’ personal information. *Fed. Aviation Admin. v. Cooper*, 566 U.S. 284, 287 (2012). The Privacy Act applies only to individuals, not corporate or government entities. 5 U.S.C. §552a(g)(1)(D) (authorizing a cause of action for adversely affected “individuals”); *id.*, §552a(a)(2) (defining “individual” as “a citizen of the United States or an alien lawfully admitted for permanent residence.”). Section (g) of the Privacy Act provides for a limited subset of civil remedies, and Plaintiffs are not individuals, and their allegations do not fall within these carefully demarcated limits of the statute. Civil remedies are available—and thus the United States’ sovereign immunity has been waived—in four circumstances: (1) when the agency “makes a determination . . . not to amend an individual’s record in accordance with his request,” (an “Amendment Action”), 5 U.S.C. § 552a(g)(1)(A), (2) when the agency refuses to comply with an individual’s request for access to her records, (an

“Access Action”), *id.* § 552a(g)(1)(B), (3), when the agency fails to maintain an individual’s records “with such accuracy, relevance, timeliness, and completeness” as is necessary for a government action and “consequently a determination is made which is adverse to the individual,” (a “Benefits Action”), *id.* § 552a(g)(1)(C), or (4) where the government “fails to comply with any other provision of this section . . . in such a way as to have an adverse act on an individual,” (an “Other Action”) *id.* § 552a(g)(1)(D). For Benefits Actions or Other Actions, a plaintiff may be liable for “actual damages sustained by the individual as a result of the refusal or failure,” subject to a \$1,000 statutory minimum, but only if the “agency acted in a manner which was intentional or willful” and if that plaintiff could prove “actual damages,” which is “limited to proven pecuniary or economic harm.” *Cooper*, 566 U.S. at 291, 299.

As to injunctive relief specifically, the Act allows for injunctive relief in only two narrow circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records of an individual, 5 U.S.C. § 552a(g)(1)(A), (g)(2)(A); and (2) to order an agency to allow an individual access to his records, *id.* § 552a(g)(1)(B), (g)(3)(A). Injunctive relief, as the D.C. Circuit has recognized, is not available for any other situation arising out of the Privacy Act. *See Sussman v. U.S. Marshal Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007) (“We have held that only monetary damages, not declaratory or injunctive relief, are available to § 552a(g)(1)(D) plaintiffs”) (citing *Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988)); *see also Cell. Assocs., Inc. v. Nat’l Insts. of Health*, 579 F.2d 1155, 1161–62 (9th Cir. 1978).

Given the Privacy Act’s comprehensive remedial scheme, courts have repeatedly recognized that “a plaintiff cannot bring an APA claim to obtain relief for an alleged Privacy Act violation.” *Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014); *see also Tripp v. Dep’t of Defense*, 193 F. Supp. 2d 229, 238 (D.D.C. 2002); *Poss v. Kern*, No. 23-cv-2199

(DLF), 2024 WL 4286088, at *6 (D.D.C. Sept. 25, 2024) (citing cases). That is consistent with the principle that “[w]here [a] ‘statute provides certain types of equitable relief but not others, it is not proper to imply a broad right to injunctive relief.’” *Parks v. IRS*, 618 F.2d 677, 84 (10th Cir. 1980) (citing *Cell. Assocs.*, 579 F.2d at 1161-62). This is especially true with the Privacy Act because Congress “link[ed] particular violations of the Act to particular remedies in a specific and detailed manner[,]” which “points to a conclusion that Congress did not intend to authorize the issuance of [other] injunctions.” *Cell. Assocs.*, 579 F.2d at 1158-59.

Indeed, as the Ninth Circuit concluded, were injunctive relief available for violations of the Privacy Act generally, “the detailed remedial scheme adopted by Congress would make little sense. We think it unlikely that Congress would have gone to the trouble of authorizing equitable relief for two forms of agency misconduct and monetary relief for all other forms if it had intended to make injunctions available across the board.” *Id.* at 1160. Plaintiffs’ efforts to obtain an agency-wide injunction on both information sharing and personnel actions by channeling Privacy Act claims through the APA would be an end run around these common-sense principles and should be rejected.

That end-run would be especially intolerable here, where Plaintiffs are not entitled to bring Privacy Act claims because they are not individuals within the meaning of the Act. Plaintiffs cannot use the APA to circumvent Congress’ deliberate choice to limit the reach of the Privacy Act only to individuals. Congress intended the remedies under the Privacy Act to be narrow, as demonstrated by the carefully reticulated scheme to limit available remedies. And on top of that scheme, and unlike other statutes such as the Freedom of Information Act, Congress chose to give a right of action only to United States persons. Allowing Plaintiffs to invoke the Privacy Act

through the APA would render the statute's limited reach meaningless, and would undo Congress' specific intent to exclude non-individual plaintiffs from its reach.

2. Internal Revenue Code

For similar reasons, it would be inappropriate to allow Plaintiffs to use the APA to create an end-run around the remedial scheme provided in the Internal Revenue Code for violations of 26 U.S.C. § 6103. Congress created a waiver of sovereign immunity for violations of § 6103 by authorizing only civil damages against the United States in 26 U.S.C. § 7431. Specifically, § 7431 authorizes a right of action against the United States if “any officer or employee of the United States knowingly, or by reason of negligence, . . . discloses any return or return information . . . in violation of section 6103.” 26 U.S.C. § 7431(a)(1). Damages are authorized in the sum of “the greater of” (a) \$1,000 for each unauthorized disclosure of a return or return information, or (b) the actual damages sustained by the plaintiff plus punitive damages for willful disclosures or disclosures that result from gross negligence. *Id.* § 7431(c). Civil damages under § 7431 is the sole remedy that Congress provided for a violation of § 6103, and it does not authorize injunctive relief. *See generally id.*; *see also Henkell v. United States*, No. 96-2228, 1998 WL 41565, at *5 (E.D. Cal. Jan. 9, 1998) (explaining that § 7431 does not authorize injunctive relief).¹

Given the civil damages available to individuals whose return information is disclosed in violation of § 6103—which is part of the complex statutory scheme Congress created in the Internal Revenue Code—there is another adequate remedy available, and Plaintiffs are not entitled to injunctive relief through the APA. *Cf. Agbanc Ltd. v. Berry*, 678 F. Supp. 804, 807 (D. Ariz.

¹ In addition, however, Congress has imposed criminal penalties for willful violations of § 6103, which are punishable as a felony and by dismissal from Federal service. 26 U.S.C. § 7213(a)(1).

1988) (concluding that § 7314 provides an adequate remedy at law that precludes equity jurisdiction).

* * *

Congress’s creation of comprehensive remedial schemes in the Privacy Act and the Internal Revenue Code, as discussed above, forbid the relief Plaintiffs seek under the APA. The APA’s waiver of sovereign immunity does not apply “if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought.” 5 U.S.C. § 702. As the Supreme Court has stated, the purpose of this carve-out waiver is to prevent plaintiffs from exploiting the APA’s waiver to evade limitations on suit contained in other statutes. *See Match-E-Be-Nash-She-Wish Band of Pottawatomis Indians v. Patchak*, 567 U.S. 209, 215 (2012). “When Congress has dealt in particularity with a claim and has intended a specified remedy—including its exceptions—to be exclusive, that is the end of the matter; the APA does not undo the judgment.” *Id.* Just so here. Congress has set out the exclusive remedies for violations of the Privacy Act and in the Internal Revenue Code in the respective statutes. The APA does not provide a waiver of sovereign immunity to evade those considered judgments.

iii. Plaintiffs have not shown a violation of any statute.

Plaintiffs’ APA claims premised on their allegation that the access policy exceeds statutory authority and is contrary to law (and their *ultra vires* and Take Care arguments, which are premised on the same purported violations), ECF No. 4 at 22-25, also fail. Plaintiffs’ legal theory is largely premised on two incorrect facts. First, they appear to claim that granting access to Treasury SGEs is “unauthorized,” because SGEs, as a class, are not entitled to access Treasury data. But as discussed below, the statutes Plaintiffs cite do not distinguish among SGEs, political appointees, or career civil servants: they apply to *employees writ large*. And Treasury SGEs are employees of

the Department of the Treasury. *See, e.g.*, 18 U.S.C. § 202 (“the term ‘special Government employee’ shall mean an officer or *employee* of the executive . . . branch of the United States Government” who serves subject to specific timing restrictions). Second, Plaintiffs claim that Treasury had a policy of restricting access to its systems only to career civil servants. However, no such policy ever existed—indeed, contractors and persons at other entities, like the Federal Reserve Bank of Kansas City have access. Thus, no such policy was changed.

In any event, the specific statutes Plaintiffs point to do not prohibit—or in most cases, even apply—to Plaintiffs themselves, much less the conduct that they challenge.

1. Privacy Act of 1974.

Plaintiffs first identify the Privacy Act as a potential statutory violation. *See* ECF No. 4 at 18. But, as discussed above, the Privacy Act, by its terms, applies only to “records” maintained by an agency about an “individual.” 5 U.S.C. § 552a(a)(4); *id.* § 552a(a)(2) (defining “individual”). In other words, the Privacy Act *only* applies and protects information of certain natural persons; it does not apply to information of a non-corporeal State. Plaintiff States claim standing based only on State information that is collected by Treasury, ECF No. 4 at 13, and they sue as states. No individuals are at issue. Accordingly, Treasury has not violated the Privacy Act because the Privacy Act does not apply to the States’ information and the States have no legal remedy under the Privacy Act.

Plaintiffs have also not plausibly alleged that a violation of the Privacy Act has occurred, even assuming (counterfactually) that their data is protected by that law. Plaintiffs first offer that, of the Privacy Act’s 13 exceptions to the general disclosure bar, “none can be reasonably construed to permit disclosure to [Special Government Employees] or political appointees who have no “need for the record in the performance of their duties.” ECF No. 4 at 18 (quoting 5 U.S.C.

§ 552a(b)(1)). That statement is a truism—plainly, an employee who has “no need” as described at § 552a(b)(1) does not qualify for the exception. But the Treasury DOGE Team members, or other future political appointees or SGEs who may do the work that Plaintiffs seek to block from access—are “officers” or “employees” of the Treasury Department, who “have a need for the records in the performance of their duties.”² *See* Krause Decl. ¶ 2 (explaining need). And to the extent Plaintiffs attempt to distinguish “special Government employees” and “political appointees” from “officers and employees” within the meaning of the Privacy Act, that distinction is unconvincing and finds no basis in law. The Act applies to “employees,” without qualification. 5 U.S.C. § 552a(b)(1). Special Government employees, after all, are “officer[s] or employee[s] of the executive or legislative branch of the United States Government, of any independent agency of the United States or of the District of Columbia, who [are] retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days, temporary duties either on a full-time or intermittent basis[.]” 18 U.S.C. § 202(a). While Plaintiffs fail to define “political appointees,” this term is commonly used to refer to excepted service positions hired under Schedule C of the Civil Service Regulations, for positions of a confidential or policy-determining character. *See* 5 U.S.C. § 2103; 5 C.F.R. § 213.3301. These employees are also considered to be “appointed in the civil service” and are “employees” of the federal government. *See* 5 U.S.C. §§ 2103, 2105.

² Marko Elez was also a Treasury employee. *See* Krause Decl. ¶ 8. Because he has departed the Treasury Department, *id.*, he cannot be the cause of any of the future harms Plaintiffs predict. *See Shain v. Ellison*, 356 F.3d 211, 215 (2d Cir. 2004) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983)).

Plaintiffs also invoke the requirement that an agency “publish in the Federal Register upon establishment or revision a notice of the existence and character of [a] system of records,” 5 U.S.C. § 552a(e)(4), to include “each routine use of the records contained in the system, including the categories of users and the purpose of such use,” *id.* § 552a(e)(4)(D). Defendants have not violated this requirement; with respect to the payment systems administered by BFS, the relevant notice was published almost five years ago. *See Privacy Act of 1974; System of Records*, 85 Fed. Reg. 11,776 (Feb. 27, 2020). And in any event, that notice is irrelevant here: the Privacy Act requires a notice of routine use to be published in advance of disclosure *outside* the relevant agency, 5 U.S.C. § 552a(b), but because the Treasury DOGE Team members were Treasury employees, there has been no such disclosure. Rather, the Privacy Act’s general authorization for intra-agency information sharing in furtherance of that employees’ duties, *see* 5 U.S.C. § 552a(b)(1), applies.

2. E-Government Act of 2002.

Plaintiffs’ allegations concerning section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. at 2921-22, codified at 44 U.S.C. § 3501 note (“EGA”), fare no better. That provision requires that the agency take certain actions before “developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form.” *Id.* § 208(b)(1)(A)(i); *see* ECF No. 4 at 18. One of those required actions is the completion of a “privacy impact assessment.” *Id.* § 208(b)(1)(B)(i). Plaintiffs claim that Defendants violated the E-Government Act by failing to conduct a privacy impact assessment before granting access to Mr. Krause and Mr. Elez. This claim fails for three reasons.

First, the E-Government Act provides no private right of action, and the APA does not provide a cause of action, because the creation of a Privacy Impact Assessment (“PIA”) does not constitute final agency action. Courts repeatedly have held that agency reports, opinions, press

releases, and similar publications do not constitute final agency action under the APA because they impose no obligation, deny no right, nor fix a legal relationship. *See, e.g., Trudeau v. FTC*, 456 F.3d 178, 189 (D.C. Cir. 2006) (finding issuance of a press release not to constitute final agency action under the APA.)

Second, the Treasury Department has not undertaken an activity that might trigger the E-Government Act. By its terms, this requirement applies only before the agency begins “developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form,” *id.* § 208(b)(1)(A)(i), or “initiating a new collection of information,” *id.* § 208(b)(1)(A)(ii). But there are no allegations that Treasury has developed or procured a new information technology system, nor begun to collect information in a new manner. Instead, Plaintiffs allege that Defendants facilitated access for two individual employees to *existing* information technology and systems.

Third, the E-Government Act does not implicate the interests of States, even if those States have sensitive information. As the D.C. Circuit has repeatedly observed, the E-Government Act protects *individual* privacy—a term inapplicable to States. *See Elec. Privacy Info. Ctr. v. U.S. Dep’t of Comm.*, 928 F.3d 95, 103 (D.C. Cir. 2019); *Elec. Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity*, 878 F.3d 371, 378 (D.C. Cir. 2017); EGA § 208 (“The purpose of this section is to ensure sufficient protections for the privacy of *personal* information as agencies implement *citizen-centered* electronic Government.” (emphases added)); *id.* § 208(b)(1)(A)(i) (triggering the privacy impact assessment requirement for information in “identifiable form,” which means “information that permits the identity of an individual,” *id.* § 208(d)); *id.* § 208(b)(1)(A)(ii)(II) (“information in an identifiable form permitting the physical or online

contacting of a specific individual” (emphasis added)). For all of these reasons, the E-Government Act does not apply at all (much less has it been violated here).

3. Internal Revenue Code.

Plaintiffs also rely on the set of statutory protections applicable to tax returns. *See, e.g.*, ECF No. 4. at 19 (citing 26 U.S.C. § 6103). Unlike the first two statutes cited by Plaintiffs, 26 U.S.C. § 6103(a), which establishes a general rule of confidentiality for tax-related “[r]eturns and return information,” may apply to information submitted by (and pertaining to) States. But that fact is not dispositive, as an exception to the general rule of § 6103(a) applies for “[d]isclosure to certain Federal officers and employees for purposes of tax administration.” *Id.* § 6103(h). Indeed, “officers and employees of the Department of the Treasury” may obtain returns and return information if their “official duties require such inspection or disclosure for tax administration purposes.” *Id.* “Tax administration,” in turn, is defined to include “the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws.” *Id.* § 6103(b)(4)(A)(i). The payment systems at issue in this case disburse the vast majority of government payments, including tax refunds. *See* Fiscal Service Overview, *available at* <https://www.fiscal.treasury.gov/about.html> (last visited Feb. 11, 2025).

The Treasury DOGE Team satisfied these statutory conditions for access to returns and return information. They were, to start, employees of the Treasury Department. Krause Decl. ¶¶ 1-2. And their “official duties” included serving as Treasury DOGE Team members who were “spearheading advances in Treasury’s technology infrastructure, financial management systems, and cybersecurity initiatives,” “overseeing the modernization of Treasury’s legacy systems,” and “collaborating with Treasury’s Chief Information Officer (CIO) to help strengthen Treasury’s cybersecurity protocols to protect its critical financial systems and mitigate risks.” *Id.* ¶ 2. Indeed,

some of the duties the Treasury DOGE team's duties related to GAO concerns regarding Improper Earned Income Tax Credit refunds. Krause Decl. ¶ 8. Moreover, the returns and return information subject to the protections of § 6103 pass through (and are stored on) the very same systems that is the Treasury DOGE Team is responsible for improving. They therefore had the requisite need to obtain § 6103 material in the exercise of their official duties.

4. Social Security Regulations.

Similarly, Plaintiffs point to the Treasury Department's regulation governing "collection, use, disclosure, and protection of [Social Security numbers]." *See* ECF No. 4 at 19 (citing 31 C.F.R. § 1.32(d)). However, Plaintiffs ground their motion for injunctive relief based on their own interests, not their citizens', ECF No. 4 at 11, and States are not assigned Social Security numbers. *See* 20 C.F.R. § 422.104(a). Because the States do not have interests within the zone protected by the relevant regulation, they lack a cause of action to establish this violation. *See Moya v. U.S. Dep't of Homeland Sec.*, 975 F.3d 120, 131-32 (2d Cir. 2020).

Regardless, Plaintiffs have not alleged a violation of the regulation. 31 C.F.R. § 1.32 contains a range of discrete parameters. *See generally* 31 C.F.R. § 1.32. Of those, the States invoke only one: the requirement that, "[w]henver feasible," the Department "mask, or truncate/partially redact Social Security numbers visible to authorized Treasury/component information technology users so they only see the portion (if any) of the Social Security number required to perform their official Treasury duties." *Id.* § 1.32(d). Despite Plaintiffs' protestations, The Treasury DOGE Team members' access was "required to perform their official duties"; namely, managing improvements to the BFS systems.

5. Title 18 Ethics Rules.

Finally, Plaintiffs note that 18 U.S.C. § 208 establishes civil and criminal penalties for government employees, including special Government employees, who participate in an official capacity in transactions in which they or a close relative or associate has a financial interest. *See* ECF No. 4 at 19-20. Once again, Plaintiffs' claim fails at the threshold, as they do not have personal interests protected by a criminal statute. *See Moya v. Dep't of Homeland Security*, 975 F.3d 120, 131-32 (2d Cir. 2020); *cf. Doe v. Broderick*, 225 F.3d 440, 447-48 (4th Cir. 2000) ("The Supreme Court historically has been loath to infer a private right of action from 'a bare criminal statute,' because criminal statutes are usually couched in terms that afford protection to the general public instead of a discrete, well-defined group." (citations omitted)).

Plaintiffs' claim fails on the merits as well. Plaintiffs recite, and Defendants do not dispute, that 18 U.S.C. § 208 generally applies to Mr. Krause, who is a special Government employee. Wenzler Decl. ¶ 4; *see* 18 U.S.C. § 208(a). Plaintiffs go on to observe that under § 208(b)(3), a special Government employee serving on an advisory committee (an irrelevant category that does not include Mr. Krause) might obtain waiver of the prohibition under certain circumstances. What the import of these facts is, Plaintiffs do not say. Instead, they conclude with a non-sequitur, averring that § 208 "does not authorize disclosure to a [special Government employee] without such a certification, yet such disclosures have been made to DOGE team members." ECF No. 4 at 20. It is not apparent what "disclosure" Plaintiffs refer to; insofar as they mean to describe disclosures of State-specific data via access to the BFS payment systems, § 208 has nothing at all to say about data disclosure. *See generally* 18 U.S.C. § 208. Similarly, § 208(b)(3) would not authorize disclosures otherwise forbidden; rather, by its very terms, it can only exempt an employee from penalties for engaging in otherwise-prohibited transactions. Far from stating a

claim of a violation of § 208, Plaintiffs have not established that this section is implicated whatsoever by the “access policy” they challenge.

iv. Plaintiffs have not identified arbitrary or capricious agency action.

Plaintiffs have also failed to show a likelihood of success on their claim that Defendants acted arbitrarily or capriciously. The gravamen of Plaintiffs’ argument is that by “changing a longstanding policy protecting PII and sensitive financial information within days of being sworn in,” Secretary Bessent acted in violation of the obligation to engage in “reasoned decisionmaking.” ECF No. 4 at 20-21. Factually, this claim misses the mark—as the Gioeli Declaration explains, Treasury is not aware that a policy limiting BFS payment system access to career employees at Treasury ever existed. Gioeli Decl. ¶ 23. That is so even if special Government employees (or even political appointees) never previously had access to the systems. To qualify as a “practice” or “policy,” an agency’s behavior must evince that it intentionally pursued the course of action previously followed. This factor distinguishes the present case from *Saget v. Trump*, 375 F. Supp. 3d 280 (E.D.N.Y. 2019), which Plaintiffs cite (at 21). *Saget* surveys various cases discussing informal agency practices, all of which demonstrate the requisite intentionality. *Id.* at 354-59. Here, the Treasury Department has never chosen to exclude special Government employees or political appointees from BFS system access; *Saget* is therefore inapposite.

Finally, to the extent the Treasury Department was required to explain its (nonexistent) change in position, it has done so here. The Treasury DOGE Team was tasked by Treasury leadership with implementing technical improvements in Treasury systems. Krause Decl. ¶2. They had good reason, then, to have access to BFS payment systems, even if others might have managed the Treasury’s systems differently. *See Islander E. Pipeline Co. v. McCarthy*, 525 F.3d 141, 150 (2d Cir. 2008).

v. Plaintiffs have not shown *ultra vires* agency action.

Plaintiffs also purport to bring a non-APA or common law *ultra vires* claim that Treasury officials acted “beyond delegated authority.” ECF No. 4 at 22 (relying on *Larson v. Domestic & Foreign Comm. Corp.*, 337 U.S. 682, 689 (1949)). Even assuming the common-law *ultra vires* doctrine still exists in suits against the federal government, *but see Apter v. Dep’t of Health & Human Servs.*, 80 F.4th 579, 593 (5th Cir. 2023) (“[U]nder our precedent, Congress apparently ‘did away with the *ultra vires* doctrine and other fictions surrounding sovereign immunity’ when it amended the APA in 1976) (quoting *Geyen v. Marsh*, 775 F.2d 1303, 1307 (5th Cir. 1985)), Plaintiffs admit that their non-APA *ultra vires* arguments are the same as their APA “exceeds statutory authority” arguments, *see* ECF No. 4 at 22. Those arguments fail for the reasons discussed above.

vi. Plaintiffs have not shown a violation of the separation of powers.

Plaintiffs’ constitutional arguments fare no better. Plaintiffs argue that the Treasury Department’s granting of employee access to Treasury Department systems somehow is a structural violation of the Constitution’s separation of power principles. ECF No. 4 at 22-24. It is not. To the contrary, it is the Plaintiffs who seek to unconstitutionally impede the President from using Executive Branch employees to implement his policy objectives.

As a threshold matter, Plaintiffs’ failed statutory claims cannot be repackaged as constitutional violations. *Dalton v. Specter*, 511 U.S. 462, 473 (1994) (“[C]laims simply alleging that the President has exceeded his statutory authority are not ‘constitutional’ claims[] subject to judicial review.”). Moreover, stripped of its rhetoric, Plaintiffs’ claim is that the Constitution prevents the Executive from “block[ing] payments to States and their residents of federal funds that have been appropriated by Congress.” *Id.* at 24. But whatever the merits of this argument,

nothing of the sort has occurred here. Plaintiffs do not plead that any payments to which they are entitled have been blocked—much less that such payments were blocked via the actions challenged in this lawsuit. This claim is therefore unripe. *See Nat'l Org. for Marriage, Inc. v. Walsh*, 714 F.3d 682, 687 (2d Cir. 2013) (“A claim is not ripe if it depends upon ‘contingent future events that may not occur as anticipated, or indeed may not occur at all.’”) (citation omitted). As a result, Plaintiffs are not likely to succeed on this claim.

vii. Plaintiffs have not shown a violation of the Take Care Clause.

Likewise, Plaintiffs’ allegation that the challenged actions violate Article II’s Take Care Clause lacks merit. At the outset, “[w]hether claims brought directly under the Take Care Clause are even justiciable is open to debate.” *Citizens for Responsibility & Ethics in Washington v. Trump*, 302 F. Supp. 3d 127, 130 (D.D.C. 2018). But this Court need not resolve that issue to reject this claim—because again, Plaintiffs admit that this argument merely puts constitutional gloss on their APA statutory authority arguments, which fail for the same reasons discussed above. ECF No. 4 at 25.

a. Plaintiffs have not shown irreparable harm.

For all of the reasons Plaintiffs have failed to show cognizable injury for the purposes of Article III standing, they have necessarily failed to show any irreparable injury, the “single most important prerequisite for the issuance of a preliminary injunction.” *Faiveley Transport Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quotation omitted); *see supra* Part I.

b. A preliminary injunction would not serve the public interest.

As the Krause Declaration, and GAO reports to which it refers, detail, there are important reasons to improve and modernize BFS systems to avoid making improper or fraudulent payments on the order of billions of dollars. Krause Decl. ¶¶ 7-9. The Treasury DOGE Team’s efforts, as

led by Mr. Krause, are intended to assess and reform the technical systems so as to improve their ability to prevent this misspending of federal funds. There is plainly a public interest served by enabling them to do so. There is also a strong public interest in the President, duly elected, implementing through Executive Branch departments the policy objectives he was elected to implement.

Against these public interests, Plaintiffs offer only a rehash of their unconvincing arguments regarding irreparable harm and likelihood of success on the merits. ECF No. 4 at 26-27. As described above, Plaintiffs have not even shown injury sufficient for standing, much less irreparable harm. As for their arguments about likelihood of success, Plaintiffs' invitation to collapse the traditional preliminary injunction inquiry into the first prong alone is an approach the Supreme Court has repeatedly rejected. *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 311-313 (1982) (overturning a preliminary injunction granted solely on the basis of likelihood of success); *Starbucks Corp. v. McKinney*, 602 U.S. 339, 346 (2024). Even if likelihood of success were the sole criterion that mattered, however, that alone should result in the motion's denial. *See supra*.

c. The Court lacks authority to enter relief directly against the President.

Plaintiffs have named President Trump as a defendant. Compl. ¶ 38. But “[w]ith regard to the President, courts do not have jurisdiction to enjoin him . . . and have never submitted the President to declaratory relief.” *Newdow v. Roberts*, 603 F.3d 1002, 1013 (D.C. Cir. 2010) (citations omitted); *see Franklin v. Massachusetts*, 505 U.S. 788, 802-03 (1992) (“[I]n general this court has no jurisdiction of a bill to enjoin the President in the performance of his official duties.”); *id.* at 827 (Scalia, J., concurring in part) (“[W]e cannot issue a declaratory judgment against the President.”); *Mississippi v. Johnson*, 71 U.S. (4 Wall.) 475, 501 (1866). Accordingly, if the Court were to grant additional injunctive relief (which it should not do), it should exclude the President

from the scope of its order. *See, e.g., U.S. Navy SEALs 1-26 v. Biden*, 578 F. Supp. 3d 822, 829 (N.D. Tex. 2022); *Oklahoma v. Biden*, 577 F. Supp. 3d 1245, 1254 (W.D. Okla. 2021).

CONCLUSION

For the foregoing reasons, the Court should deny Plaintiffs' motion for a preliminary injunction.

Dated: February 11, 2025

BRETT A. SHUMATE
Acting Assistant Attorney General
Civil Division

JOHN R. GRIFFITHS
Director
Federal Programs Branch

/s/ Bradley P. Humphreys
BRADLEY P. HUMPHREYS
(D.C. Bar No. 988057)
Senior Trial Counsel
Federal Programs Branch
Civil Division, Department of Justice
1100 L Street NW
Washington, DC 20005
Telephone: (202) 305-0878
Bradley.Humphreys@usdoj.gov

Respectfully submitted,

DANIELLE R. SASSOON
United States Attorney

By: /s/ Jeffrey Oestericher
JEFFREY OESTERICHER
REBECCA S. TINIO
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, NY 10007
Telephone: (212) 637-2695/2774
Email: jeffrey.oestericher@usdoj.gov
rebecca.tinio@usdoj.gov

Certificate of Compliance

Pursuant to Local Civil Rule 7.1(c), the above-named counsel hereby certifies that this memorandum complies with the word-count limitation of this Court's Local Civil Rules. As measured by the word processing system used to prepare it, this memorandum contains 11730 words.