UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

STATE OF NEW YORK, STATE OF ARIZONA, STATE OF CALIFORNIA, STATE OF COLORADO, STATE OF CONNECTICUT, STATE OF DELAWARE, STATE OF HAWAII, STATE OF ILLINOIS, STATE OF MAINE, STATE OF MARYLAND, COMMONWEALTH OF MASSACHUSETTS, STATE OF MINNESOTA, STATE OF NEVADA, STATE OF NEW JERSEY, STATE OF NORTH CAROLINA, STATE OF OREGON, STATE OF RHODE ISLAND, STATE OF VERMONT, and STATE OF WISCONSIN, Plaintiffs, v. DONALD J. TRUMP, IN HIS OFFICIAL CAPACITY AS PRESIDENT OF THE UNITED STATES; U.S. DEPARTMENT OF THE TREASURY; and SCOTT BESSENT, IN HIS OFFICIAL CAPACITY AS SECRETARY OF U.S. DEPARTMENT OF THE TREASURY, Defendants.	C.A. No. 25-cv-1144 (JAV)

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

TABLE OF CONTENTS

INTRODUCTION

1. The U.S. Treasury Department ("Treasury") has been a storied institution of this Country since its founding. Established by an act of Congress and first led by Alexander Hamilton, Treasury oversees the nation's financial system: it manages federal finances, collects taxes, pays the government's bills, and otherwise maintains the responsibility of protecting, accounting for, and disbursing of our national finances and debts.

2. Treasury executes its functions utilizing and relying upon highly protected information systems and data concerning our federal finances. These systems and data contain sensitive information concerning the many states of this Country, as well as their residents.

3. For decades, there have been policies in place to protect Treasury's highly sensitive systems and data from mishandling, inappropriate use and access, as well as to prevent security breaches that would cause harm to such sensitive information and those to whom it belongs.

4. Since January 21, 2025, the executive branch, including Treasury and Treasury Secretary Scott Bessent ("Secretary"), have ignored these policies in order to implement a rushed and chaotic plan that requires granting broad systems and data access to new and insufficiently vetted and trained Treasury employees, upending the protections of such sensitive information under the pretext that unspecified "fraud, waste, and abuse" can be rooted out of the federal financial systems.

5. Plaintiffs the States of New York, Arizona, California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maine, Maryland, Minnesota, Nevada, New Jersey, North Carolina, Oregon, Rhode Island, Vermont, and Wisconsin, and the Commonwealth of Massachusetts (collectively "States") bring this action 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 U.S. Department of the Treasury ("Defendants"), to end Defendants' unlawful violation of federal information security requirements in furtherance of illegal ideological screening of payment disbursals. The States seek declaratory and injunctive relief enjoining Defendants from (1) permitting unrestrained access to the States' sensitive and confidential financial information in violation of federal laws and regulations governing information security; and (2) changing Treasury's historic policy and practice relating to the review of payment requests for appropriated funds to allow an automated process at Treasury to pause and potentially block disbursements to the States impermissibly based on ideology.

6. The States' injuries from the unprecedented access to Treasury's systems and the States' data are twofold. First, Treasury, by its own admissions, has put the States' confidential information at serious risk through shoddy and insufficient training, vetting, oversight, and hiring procedures—in contravention of federal law and regulations governing information security—and even shoddier execution. Second, Treasury's stated goal, through a new automated review process, of pausing and potentially blocking the disbursement of congressionally appropriated funds to the States based on ideological criteria driven by the President's executive orders will harm the States' fiscs by causing them to outlay funds for federal programs in anticipation of reimbursement that will be at a minimum delayed, and possibly blocked, for entirely unlawful reasons.

7. Specifically, these harms stem from two discrete actions by Treasury.

8. First, Treasury has put into place a hybrid team of employees, working on behalf of the President's newly created Department of Government Efficiency ("DOGE"), led by Elon Musk, to perform functions aimed at achieving the goals outlined in several presidential executive orders. Treasury and Secretary Bessent have granted these hybrid DOGE-Treasury employees

expanded access to the sensitive information contained in the Treasury systems and data, including within the Bureau of the Fiscal Services ("BFS"), belonging to the States.

9. Defendants did so without following federally-mandated information security policies, a failure that poses huge cybersecurity risks, including risks to the States and their residents that their information will be used and processed, unchecked, in a manner not permitted by federal law—an outcome that has, by the Defendants' own admission, already occurred when a member of the DOGE-Treasury team sent confidential Treasury information to federal employees outside of Treasury.

10. Furthermore, members of Congress[1] and numerous media reports have raised concerns that data from other federal agencies is being fed into an open-source Artificial Intelligence ("AI") system owned and controlled by a private third party, without measures taken to ensure the privacy and security of the States' data,[2] or even consideration of whether the law permits any commercial access to the data, no matter how secure. The third-party cloud computing

[1] Letter from Members of Congress to the Hon. Russell Vought dated April 16, 2025, available at https://beyer.house.gov/uploadedfiles/congressional_letter_to_administration_on_doge_use_of_ai.pdf.

[2] Molly Bohannon. *Trump Vs. Education Department: McMahon Says She'll Keep Pell Grants, Title I—As Trump Pushes to Shelter DOE*, Forbes (Feb. 13, 2025), https://www.forbes.com/sites/mollybohannon/2025/02/13/trump-vs-education-department-mcmahon-says-shell-keep-pell-grants-title-i-as-trump-pushes-to-shutter-doe/; Alexandra Ulmer et al., *Musk's DOGE using AI to snoop on U.S. federal workers, sources say*, Reuters (Apr. 8, 2025), https://www.reuters.com/technology/artificial-intelligence/musks-doge-using-ai-snoop-us-federal-workers-sources-say-2025-04-08/.

service that DOGE is reportedly using for this effort has experienced at least one major security breach.[3]

11. Upon information and belief, the access Defendants have granted, and will continue to grant, DOGE-Treasury employees to the States' confidential information is in furtherance of the unlawful data pooling that DOGE has undertaken at other federal agencies.

12. Second, upon information and belief, Treasury has altered its decades of agency practice and policy to entirely upend Treasury's historic ministerial function of disbursing payments under appropriated federal programs, and instead has instituted a new policy, using an automated system being developed by DOGE-Treasury employees, to pause and potentially block disbursement of appropriated funds on ideological grounds.

13. This new process for reviewing on ideological grounds payment requests for federal program funds is a marked departure from longstanding Treasury policy. As acknowledged by Treasury, Treasury's role has, historically, been ministerial when it comes to processing payments to the States: "the agency responsible for making the payment always drives the payment process."[4] There is no reasoned explanation for this change in policy; rather, the only explanation provided is that the policy change is necessary for the unlawful purpose of carrying out the dictates of executive orders seeking to block payments appropriated and authorized by Congress, merely because they do not align with the administration's prerogatives.

---

[3] Anuj Mudaliar, *Azure and Microsoft Exchange Servers Victim to Active Exploitation by Hackers,* Spiceworks (Feb. 21, 2024), https://www.spiceworks.com/it-security/vulnerability-management/news/azure-microsoft-exchange-servers-active-exploitation-hackers/.

[4] U.S. Dep't of Treasury, *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), https://home.treasury.gov/news/press-releases/sb0009.

14. The States suffer great harm from Defendants' use of confidential information to create a new process for ideological review of payments, as it puts vast amounts of federal funding for the States and their residents in peril. For many of the federal programs at issue here, the States pay recipients of these funds directly from their respective treasuries, and the States are then reimbursed by the relevant federal agency via a payment disbursed by Treasury. Now, States face the risk, already realized in disputes with the federal government in separate ongoing litigation, that the States will be left holding the proverbial bag for the federal government until such time as Treasury issues reimbursement after delay, if ever.

15. The States are entitled to relief on multiple grounds. First, Defendants' failures to abide by federally mandated information security requirements, placing the States' confidential financial information at risk, violate the Administrative Procedure Act's ("APA") prohibitions on agency action that is arbitrary and capricious or contrary to law. Second, Treasury's change in policy for reviewing federal program payment requests from a ministerial review process to a substantive review process based on ideological grounds is also both arbitrary and capricious and contrary to law. Finally, by adopting a review process that pauses and potentially blocks federal program disbursements to the States on ideological grounds in defiance of congressional appropriation, Defendants violate both the Separation of Powers doctrine and the Take Care Clause of the United States Constitution.

JURISDICTION AND VENUE

16. This Court has jurisdiction under 28 U.S.C. § § 1331 and 2201(a). *See* 5 U.S.C. § 552a(g)(1)(D). Jurisdiction is also proper under the judicial review provisions of the APA, 5 U.S.C. §§ 702, 704.

17. An actual controversy exists between the parties within the meaning of 28 U.S.C. § 2201(a), and this Court may grant declaratory relief, injunctive relief, and other relief pursuant to 28 U.S.C. §§ 2201–2202, and 5 U.S.C. §§ 705–706.

18. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b)(2) and (e)(1). Defendants are an agency of the United States government and officers sued in their official capacities. Plaintiff the State of New York is a resident of this judicial district, and a substantial part of the events or omissions giving rise to this Complaint occurred and are continuing to occur within the Southern District of New York.

PARTIES

1. Plaintiffs

19. Plaintiff the State of New York, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is New York State's chief law enforcement officer and is authorized under N.Y. Executive Law § 63 to pursue this action.

20. Plaintiff the State of Arizona, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is Arizona's chief law enforcement officer and is authorized under Arizona Revised Statute § 41-193(A)(3) to pursue this action.

21. The State of California is a sovereign state of the United States of America. California is represented by Attorney General Rob Bonta, who is the chief law enforcement officer of California.

22. Plaintiff the State of Colorado, represented by and through its Attorney General Phil Weiser, is a sovereign state of the United States. The Attorney General acts as the chief legal representative of the state, and is authorized under section 24-31-101, C.R.S., to pursue this action.

23. Plaintiff the State of Connecticut, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is Connecticut's chief legal officer and is authorized under General Statutes § 3-125 to pursue this action on behalf of the State of Connecticut.

24. Plaintiff the State of Delaware is a sovereign state of the United States of America. This action is brought on behalf of the State of Delaware by Attorney General Kathleen Jennings, the "chief law officer of the State." *Darling Apartment Co. v. Springer*, 22 A.2d 397, 403 (Del. 1941). Attorney General Jennings also brings this action on behalf of the State of Delaware pursuant to her statutory authority. 29 Del. C. § 2504.

25. Plaintiff the State of Hawai'i, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is Hawaii's chief legal officer and chief law enforcement officer and is authorized by Hawaii Revised Statues § 28-1 to pursue this action.

26. Plaintiff the State of Illinois is a sovereign state of the United States. It is represented in this action by the Attorney General of Illinois, who is the chief legal officer of the State and is authorized to pursue this action on behalf of the State pursuant to Article V, Section 15 of the Illinois Constitution and 15 ILCS 205/4.

27. Plaintiff the State of Maine, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is Maine's chief law officer and is authorized under 5 Me. Rev. Stat. Ann. sec. 191 to pursue this action.

28. Plaintiff the State of Maryland is a sovereign state of the United States of America. Maryland is represented by Attorney General Anthony G. Brown who is the chief legal officer of Maryland.

29. Plaintiff the Commonwealth of Massachusetts, represented by and through its Attorney General, is a sovereign state of the United States. The Attorney General is the chief law officer of the Commonwealth and is authorized under Mass. Gen. Laws ch. 12, s. 3, to pursue this action.

30. The State of Minnesota is a sovereign state of the United States of America. Minnesota is represented by Attorney General Keith Ellison who is the chief law enforcement officer of Minnesota.

31. Plaintiff State of Nevada, represented by and through Attorney General Aaron D. Ford, is a sovereign State within the United States of America. The Attorney General is the chief law enforcement of the State of Nevada and is authorized to pursue this action under Nev. Rev. Stat. 228.110 and Nev. Rev. Stat. 228.170.

32. Plaintiff State of New Jersey is a sovereign state of the United States. The Attorney General of New Jersey is the State's chief legal adviser and is authorized to act in federal court on behalf of the State on matters of public concern.

33. Plaintiff the State of North Carolina is a sovereign state of the United States of America. North Carolina is represented by Attorney General Jeff Jackson who is the chief law enforcement officer of North Carolina.

34. Plaintiff the State of Oregon, represented by and through Attorney General Dan Rayfield, is a sovereign state of the United States. The Oregon Attorney General is Oregon's chief law enforcement officer and authorized to pursue this action by Oregon Revised Statutes Chapter 180. Oregon's more than 4.2 million residents have numerous contacts with federal financial systems and the Defendants have now exposed their sensitive financial information not just to individuals lacking qualifications and security clearance, but potential hostile actors and malware

attacks. In addition to the majority of Oregonians who pay taxes, residents of the State of Oregon include veterans, employees of multiple federal agencies who received their wages through federal payment systems, and vulnerable individuals participating in federal programs for children, crime victims, and persons with disabilities.

35. Plaintiff the State of Rhode Island is a sovereign state in the United States of America. Rhode Island is represented by Attorney General Peter F. Neronha, who is the chief law enforcement officer of Rhode Island.

36. The State of Vermont is a sovereign state of the United States of America. Vermont is represented by Attorney General Charity Clark, who is the chief law enforcement officer of Vermont.

37. The State of Wisconsin is a sovereign state of the United States of America. Wisconsin is represented by Attorney General Josh Kaul who is the chief law enforcement officer of Wisconsin.

2. Defendants

38. Defendant Donald J. Trump is sued in his official capacity as the President of the United States. He is responsible for the actions and decisions that are being challenged by Plaintiffs in this action.

39. Defendant the United States Department of the Treasury is a cabinet agency within the executive branch of the United States government. 31 U.S.C. § 301. Treasury is responsible for ensuring the financial security of the United States.

40. Defendant Scott Bessent is sued in his official capacity as the United States Secretary of the Treasury and in that role is responsible for the operations of Treasury and managing the finances of the United States.

LEGAL BACKGROUND

1. The Administrative Procedure Act

41. The APA permits judicial review by persons "suffering legal wrong because of agency action, or adversely aggrieved by agency action." 5 U.S.C. § 702; *see id.* § 7031.

42. The APA provides that courts must "hold unlawful and set aside" agency action that is "in excess of statutory jurisdiction, authority, or limitations"; that is "not in accordance with law"; or that is "arbitrary, capricious, [or] an abuse of discretion." 5 U.S.C. §§ 706(2)(A), (C), (D).

2. Laws and Regulations Governing Sensitive Data

43. Federal laws and regulations protect sensitive financial information from improper disclosure and misuse, including by imposing conflict of interest limitations on federal officials and requiring that agencies put in place information security measures.

a. Federal Information Security Management Act

44. The E-Government Act of 2002 recognizes the importance of information security to the economy and national security interests of the United States. 44 U.S.C. § 3501.

45. Congress passed the E-Government Act to "promote the use of the Internet and electronic government services," "to make the Federal Government more transparent and accountable," as well as "to provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws." *Id.*

46. The Federal Information Security Management Act ("FISMA") is a federal law enacted under Title III of the E-Government Act of 2002. Pub. L. 107-347 (Dec. 17, 2002).

47. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support

the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.[5]

48. FISMA was later amended by the Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (Dec. 18, 2014), to include several modifications that modernized federal security practices to address evolving security concerns. The changes, among other things, strengthened the use of continuous monitoring in systems and increased focus on the agencies for compliance and reporting that is more targeted at the issues caused by security incidents. 44 U.S.C. § 3551.

49. In support of and reinforcing FISMA, OMB through Circular A-130, *"Managing Federal Information as a Strategic Resource*," requires executive agencies within the federal government to: (i) Plan for security; (ii) Ensure that appropriate officials are assigned security responsibility; (iii) Periodically review the security controls in their systems; and (iv) Authorize system processing prior to operations and periodically thereafter. *Id.*

50. Under FISMA, the National Institute of Standards and Technology ("NIST") must set standards and best practices for information security at federal agencies, and agencies must meet security standards and conduct annual, independent evaluations of their information security. 44 USC §§ 3543–3545.[6]

---

[5] As defined in FISMA, "[t]he term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency." 40 U.S.C. § 11331(g)(1).

[6] *See also* NIST, *NIST Risk Management Framework* (updated Sept. 24, 2024) https://csrc.nist.gov/projects/risk-management/fisma-background.

51. Accordingly, under FISMA, federal agencies need to provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of an agency; [and] (ii) information systems used or operated by an agency or a contractor of an agency or other organization on behalf of an agency," in addition to "comply[ing] with the information and security standards and guidelines, and mandatory required standards developed by NIST."[7]

52. The information security requirements established by NIST are binding on all federal agencies.[8] NIST requires that federal agencies have, at a minimum, policies and procedures that address the following information security risks:

a. Access control: Each agency must establish an internal control to "[d]efine and document the types of accounts allowed and specifically prohibited for use within the system;" "[r]equire approvals by" a designated official "for requests to create accounts;" and "[m]onitor the use of accounts."[9] Each agency must ensure that "[u]sers requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access."[10]

b. Information exchange: Each agency must establish an internal control to "[a]pprove and manage the exchange of information between the system and other systems," whether through memoranda of understanding or information exchange security agreements.[11] This includes any "organization-to-organization communications," such as e-mails, and requires "[a]uthorizing officials [to] determine the risk

[7] *Id.* (cleaned up).

[8] NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, at 2 (Sept. 2020) ("The use of these controls is mandatory for federal information systems.").

[9] *Id.* at 19.

[10] *Id.*

[11] *Id.* at 86–87.

associated with system information exchange and the controls needed for appropriate risk mitigation."[12] Furthermore, each agency must have a process in place for responding to "information spillage," or "instances where information is placed on systems that are not authorized to process such information."[13]

c. Insider threats: Each agency must "[i]mplement an incident handling capability for incidents involving insider threats," and must provide for intra-organization coordination of insider threat response.[14]

d. Personnel sanctions: Each agency must "[e]mploy a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures."[15]

b. 18 U.S.C. §§ 207, 208

53. The federal government maintains a compilation of ethics laws that constitute an ethics code governing the conduct of federal employees. Title 18 of the U.S. Code provides restrictions on federal employee conduct in order to ensure such employees avoid conflicts of interest, including personal interests that affect official action. *See* 18 U.S.C. § 208(a);[16] *see also* 5 C.F.R. part 260. Special government employees are contemplated in these ethics rules, including § 208(a), and subject to penalties under § 216 of the Code. *See* 18 U.S.C. § 216 (describing the remedies for violating, *inter alia*, §§ 207 and 208, include civil penalties up to $50,000 for each

[12] *Id.* at 87.

[13] *Id.* at 158–59.

[14] *Id.* at 153–54.

[15] *Id.* at 227.

[16] This statute provides that, with some exceptions, "an officer or employee of the executive branch of the United States Government, … including a special Government employee, [who] participates personally and substantially as a Government officer or employee" in a matter "in which, to his knowledge, he, his spouse, minor child, general partner, organization in which he is serving as officer, director, trustee, general partner or employee, or any person or organization with whom he is negotiating or has any arrangement concerning prospective employment, has a financial interest—Shall be subject to the penalties set forth in section 216 of this title."

violation, or an injunction to enjoin further violations). The only exception from § 208(a)'s requirements relevant here would be for the appointing official of a special government employee ("SGE") (with a duly filed financial disclosure pursuant to chapter 5 of title 31) to review the SGE's disclosure and certify that their work "outweighs the conflict of interest." 18 U.S.C. § 207(c).

ALLEGATIONS

1. Treasury and the Bureau of the Fiscal Service

54. Treasury is an executive branch department of the United States government; it functions as the national treasury and the finance department for the federal government. 31 U.S.C. § 301. Part of Treasury's function is to collect all federal taxes through the Internal Revenue Service; manage U.S. government debt instruments; license and supervise banks and thrift institutions; and advise the legislative and executive branches on matters of fiscal policy.[17]

55. Treasury is also responsible for managing the finances of the United States Government. Its responsibilities include collecting receipts owed to the government and making payments to recipients of public funds. 31 U.S.C. §§ 3301, 3321. In fiscal year 2024, Treasury handled $6.752 trillion in disbursements.[18] Treasury is the largest collections, payments, cash management, and financial operation in the world.

[17] *See* U.S. Dep't of Treas., *Role of the Treasury*, https://home.treasury.gov/about/general-information/role-of-the-treasury.

[18] U.S. Dep't of Treas., Bur. of Fiscal Serv., *Final Monthly Treasury Statement, Receipts and Outlays of the United States Government for Fiscal Year 2024 Through September 30, 2024, and Other Periods 4*, available at https://fiscaldata.treasury.gov/static-data/published-reports/mts/MonthlyTreasuryStatement_202409.pdf.

56. Treasury is split into two main organizational components: departmental offices and operating bureaus. Treasury's departmental offices are "primarily responsible for the formulation of policy and management of the Department as a whole, while the operating bureaus carry out the specific operations assigned to the Department." *Id*.

57. BFS is one of Treasury's operational bureaus. As described in its mission statement, BFS seeks to "promote financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services."[19]

58. BFS's executive functions include (i) collecting funds: "Provid[ing] citizens a variety of modern electronic options for paying federal taxes, charges, and fees. Minimiz[ing] lockboxes and paper processing"; (ii) disbursing funds: "[c]reat[ing] a seamless end-to-end process that is all-electronic from the initiating transaction through settlement"; (iii) financing: "…offering Treasury securities to investors through modern, secure, and reliable technology"; (iv) reporting: "[p]roviding federal agencies and the American public information that is accurate, accessible, and transparent [and s]treamlining the federal reporting process to reduce agency reporting burden"; and (v) servicing: "[p]rovid[ing] customer-centric services and solutions to agencies that enable improved decision-making and high-performance through innovation, standardization, operational efficiency, and risk reduction."[20]

[19] Bur. of Fisc. Serv., *About Us* (updated Jan. 23, 2025), https://fiscal.treasury.gov/about.html.

[20] *Id.*

59. Handling 1.2 billion transactions a year, BFS disburses 90% of all federal payments.[21] BFS is responsible for providing reimbursement directly to the States for Congressionally mandated programs like the Environmental Protection Agency's Solar for All Program, which came out of the Greenhouse Gas Reduction Fund included in the Inflation Reduction Act. Pub. L. 117-169 § 60103 (Aug. 16, 2022). In doing so, BFS maintains, and is responsible for, sensitive and confidential financial information, including the States' banking account numbers, as well as confidential financial information about the amount and type of payments made to the States ("Sensitive Data").

60. BFS relies on several systems to perform its executive functions: the Payment Automation Manager ("PAM")—the primary application used by Treasury to process payments for disbursement; the Secure Payment System ("SPS")—used to certify payment files; the Automated Standard Application for Payments ("ASAP")—which allows recipients to draw down funds from established accounts; International Treasury Services.gov ("ITS")—used by federal agencies to make international payments; and the Central Accounting and Reporting System ("CARS")—used to record financial data on agency spending and enable agency reporting for accounting purposes.

61. Treasury also operates a Payment Information Repository System ("PIRS") that is a centralized system holding information on all payments that both Treasury and non-Treasury disbursing offices make.

[21] *See* U.S. Dep't of Treas., *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), https://home.treasury.gov/news/press-releases/sb0009.

62. PAM includes several component sub-systems, including the "file system," which receives payment files from payor agencies into its "landing zone," the system that ingests the payment files before agencies certify the payments for processing. Contained within the payment files is Sensitive Data, including the States' confidential banking information.

63. For BFS to issue disbursement of federal funds through these payment systems, federal agencies who owe payments to recipients outside of the federal government prepare and send to BFS a "payment file" containing the coded payment instructions for the desired disbursements after they certify that the payees are eligible to receive the funds and that the payment is proper.

64. BFS then does a limited review of the file by checking it against various "Do Not Pay" databases. Any flags generated by this check are then reviewed by the submitting agency, which then certifies or corrects the payment file for processing through SPS.

65. Because the responsible agency certifies the payment file,[22] BFS's limited historic role has been to process the disbursement of funds in accordance with the coded data in the payment file as received from the sending agency, after performing its routine fraud checks. In other words, "the agency responsible for making the payment always drives the payment process."[23]

---

[22] *See* Bur. of Fisc. Serv., *Do Not Pay* (last visited May 23, 2025) https://www.fiscal.treasury.gov/DNP/. These data sets check whether the intended payee is deceased (the "death master file"), delinquent on federal debts, or debarred from receiving payments or doing business with the federal government—such as blocked foreign nationals on the Office of Foreign Assets Control's list. If issues are flagged, it is the agency that initiated the payment file that must adjudicate them and determine whether a payment is proper.

[23] U.S. Dep't of Treas., *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), https://home.treasury.gov/news/press-releases/sb0009.

66. Housed on a secure mainframe, the BFS systems, including PAM and SPS, control government payments that in their totality amount to more than a fifth of the U.S. economy.

2. The Department of Government Efficiency

67. A stated purpose of DOGE was to "dismantle Government Bureaucracy, slash excess regulations, cut wasteful expenditures, and restructure Federal Agencies." DOGE was created by Executive Order 14,158 (the "DOGE Executive Order"), which renamed the then-existing United States Digital Service ("USDS") as the United States DOGE Service located within the Executive Office of the President.

68. The DOGE Executive Order also established "the U.S. DOGE Service Temporary Organization" within DOGE, which is "dedicated to advancing the President's 18-month DOGE agenda" through July 4, 2026, headed by the USDS Administrator who reports to the White House Chief of Staff.

69. The DOGE Executive Order also directed every federal agency to establish a "DOGE Team" of at least four employees, selected in consultation with the USDS Administrator, and to ensure that DOGE "has full and prompt access to all unclassified agency records, software systems, and IT systems."

70. On February 11, 2025, President Trump signed Executive Order 14,210 ("Second DOGE Executive Order"), which "implement[ed] the President's '[DOGE]' Workforce Optimization Initiative," directed agencies to develop data-driven hiring plans to ensure new hires are in highest-need areas, and mandated that agencies shall not fill vacancies that "the DOGE Team Lead assesses should not be filled" unless the agency determines otherwise. (Exec. Order No. 14210, 90 Fed. Reg. 9,699 (Feb. 11, 2025)).

71. A subsequent third Executive Order directed federal agencies to consult with DOGE Team Leads on contract and grant reviews, approvals, and terminations. (Exec. Order No. 14,222, 90 Fed. Reg. 11,095 (Feb. 26, 2025)).

72. Elon Musk has been identified as the leader of DOGE by the President and Musk's personal lawyers in public statements and through posts on X.com.[24] President Trump has stated that DOGE is acting at "[his] insistence" and that Musk answers to President Trump. Musk has similarly confirmed his role within and overseeing DOGE, used his personal X platform to endorse and promote DOGE, and has even stated in public appearances with President Trump his duties to execute DOGE functions at the President's direction. As of the date of this complaint, any OGE Form 278 (required by the Office of Government Ethics to address conflicts issues) that Musk has filed has not been made public.

73. In a declaration provided to the District Court of Maryland by Director of White House Office Administration Joshua Fisher, Musk's position has been described as an "employee of the White House Office with the title of Senior Advisor to the President" and that he is classified as a "Special Government Employee." Fisher stated that Musk is "not an employee of the U.S. DOGE Service or U.S. DOGE Service Temporary Organization," which are entities of the Executive Office of the President separate from the White House Office. Further, the declaration asserts that Musk is not the U.S. DOGE Service Administrator.

74. Musk has described DOGE as "a support function for the President and for the ... agencies and departments" and that "one of the biggest functions of the DOGE team is just making sure that the presidential executive orders are actually carried out."

[24] Anna Bower (@AnnaBower), X.com (May 21, 2025 3:15PM), https://x.com/annabower/status/1925269203310846404?s=46.

75. The reporting structure of DOGE employees placed in the various federal agencies, including Treasury, is unclear, even with the benefit of multiple rounds of declarations from Defendants in this action. To date, Defendants have failed to provide any clear description of the reporting lines between the DOGE-Treasury team and the wider DOGE team based out of USDS. For example, there is no clear explanation that the DOGE-Treasury team is restricted from disclosing sensitive Treasury information to DOGE teams outside of Treasury as part of their dual responsibilities.

76. Section 3(c) of the DOGE Executive Order directs federal agencies to consult with USDS, and in consultation with the USDS Administrator, to establish a DOGE team of at least four employees—which may include special government employees ("SGEs")—to embed in their agency.

77. Upon information and belief, DOGE employees are generally appointed into a schedule C transition position within the federal agency in which the DOGE team is embedded, based on the recommendation from DOGE that the agency take on the employee appointment.

78. Section 4(b) of the DOGE Executive Order imposes a duty on agency heads to "take all necessary steps, in coordination with the USDS Administrator and to the maximum extent permitted by law, to ensure USDS has full and prompt access to all" of the agency's unclassified records and IT systems.

79. While the DOGE employee embedded in an agency works within that agency, the employee also has reporting obligations and responsibilities to serve the mission and goals of DOGE.

80. Furthermore, the makeup of any given DOGE team, including the DOGE-Treasury team, is subject to rapid change. For example, Marko Elez was replaced with Ryan Wunderly at

Treasury, while Elez himself went on to join the DOGE team at Health and Human Services ("HHS"). Between the date that the Defendants in this action filed for partial dissolution of the preliminary injunction with respect to Wunderly and the filing of this complaint, another Treasury-DOGE team member who had been detailed to the IRS, Gavin Kliger, had left.

81. Although Amy Gleason is identified as the USDS Administrator, Elon Musk is the de facto head of DOGE, in addition to serving as a special advisor to the President. Musk's conflict waivers, if any, have not been publicly disseminated; however, he continues to maintain his leadership roles at his private companies, including Starlink and Tesla, while also overseeing DOGE's work.

3. Defendants' Information Security Breaches at Treasury

82. The States originally filed this action and obtained a temporary restraining order ("TRO") to restrain access by the DOGE Treasury team three weeks into the DOGE intervention at Treasury. As of that date, two DOGE members had already been embedded at Treasury and had review access to source code for BFS's payment systems and databases across multiple BFS payment systems, as well as the ability to review Sensitive Data.

83. There has already been disclosure of the States' Sensitive Data to two DOGE employees—Marko Elez and Thomas Krause—who, at the time, were not specifically authorized to view the information under governing law and regulations. Nor did they have the requisite training or vetting to entitle them to the level of access to BFS's systems that they were given.

84. On at least one occasion, Elez was mistakenly provided access to BFS systems with "read/write permissions instead of read-only." Gioeli Aff. ¶¶ 13, 20 (ECF No. 34). But even with the more restricted "read-only" access, Elez still had "the ability to view and query information and data"; in other words, he had access to the States' Sensitive Data. *Id*. ¶ 17.

85. Elez ultimately resigned from DOGE-Treasury due to news reports calling attention to his racist social media comments posted last year. During his time serving at DOGE-Treasury, Elez impermissibly accessed sensitive BFS data systems, impermissibly took screenshots of data from the system, emailed at least one spreadsheet of data to federal employees outside of Treasury, and otherwise flouted detection from Treasury security in violation of the protocols protecting Sensitive Data. Regardless of this conduct, however, Elez has been re-hired by Musk and is working for the DOGE efforts aimed at Health and Human Services.

86. There is no evidence that Elez was ever disciplined in any way for his information security failures while at Treasury, nor any indication that a review or investigation of Elez's conduct by Defendants was completed.

87. The DOGE team's prior and future access carries with it an ongoing risk—already realized by Treasury's failure to prevent Elez's information security violations and ongoing failure to take appropriate disciplinary actions against Elez—that could cause future harm by compromising the States' Sensitive Data, including "potential operational disruptions to [BFS'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." Gioeli Aff. ¶ 11 (ECF No. 34).

88. Heightening the ongoing risk of data security breaches is the DOGE-Treasury team's ongoing coordination with and "regular updates" to DOGE writ large. Defendants have thus far refused to confirm whether or not confidential information maintained in the BFS systems is shared with members of the DOGE team who are not Treasury employees.

89. The granting of access to the DOGE-Treasury team was rushed and undertaken under political pressure. PI Hearing Tr. at 18:19-23; *id.* at 19:9-11; *id.* at 53:11-13 ("[T]ime was

of the essence because the executive order made time of the essence and compliance with them made time of the essence.").

90. As this Court previously found in connection with Plaintiffs' motion for a preliminary injunction, "the launch of the Treasury DOGE Team was chaotic and haphazard," and DOGE-Treasury employees were given access to Sensitive Data "after receiving minimal, if any, training regarding the handling of sensitive government information (beyond being instructed to maintain the information on [a] BFS laptop)." *New York v. Trump*, No. 25-cv-1144, 2025 WL 573771, at *21-22 (S.D.N.Y. Feb. 21, 2025).

91. Federal law and the critical sensitivity of the information contained in the BFS payment systems, including the Sensitive Data, require more than the haphazard approach to cybersecurity demonstrated by the Defendants thus far.

92. According to public reporting, the Treasury Inspector General is investigating DOGE access within Treasury, following concerns expressed by some within the IRS that DOGE employees under Musk's direction have improperly accessed taxpayer information or shared it with other government agencies.[25]

a. DOGE Employees' Backgrounds and Conflicts of Interest Signal Information Security Vulnerability

93. According to public reporting, the DOGE team members include numerous individuals who have connections to Musk's companies, as well as his allies, including many of

[25] William Turton et al., *Inspector General Probes Whether Trump, DOGE, Sought Private Taxpayer Information or Sensitive IRS Material,* ProPublica (Apr. 25, 2025), https://www.propublica.org/article/trump-doge-irs-treasury-tigta-inspector-general-probe.

the DOGE-Treasury team members.[26]

94. Edward Coristine is a 19-year-old "expert"[27] DOGE employee detailed to the Office of Personnel Management and the General Services Administration, who previously held an internship position at Musk's Neuralink. Based on public reporting, Coristine previously interned with Path Network, a network monitoring firm reputed for hiring former "blackhat hackers," and is associated with an online handle that was solicited for a cyberattack-for-hire in 2022.[28] Path Network terminated Coristine from his internship after concluding in an internal investigation that Coristine's tenure coincided with a leak of proprietary company information.[29] Coristine bragged about sharing Path Network company secrets and access on his Discord server, stating, "I had access to every single machine," shortly after his 2022 termination.[30]

95. At least three DOGE-Treasury employees appear to have problematic conflicts that could impact the objective performance of their duties at Treasury.[31]

---

[26] Avi Asher-Shapiro et al., *Elon Musk's Demolition Crew*, ProPublica (updated May 7, 2025), https://projects.propublica.org/elon-musk-doge-tracker/.

[27] Andy Greenberg et al., *DOGE Teen Owns 'Tesla.Sexy LLC' and Worked at Startup That Has Hired Convicted Hackers*, WIRED (Feb. 6, 2025), https://www.wired.com/story/edward-coristine-tesla-sexy-path-networks-doge.

[28] *Id.*

[29] Victor Tangermann, *One of Elon Musk's DOGE Boys Was Fired by Previous Job for Leaking Company Secrets,* Yahoo News (Feb. 7, 2025), https://www.yahoo.com/news/one-elon-musks-doge-boys-203826710.html.

[30] *Id*.

[31] Michael Stratford, '*Glaring Red Flag': Treasury DOGE Team Discloses Bank Stock Holdings,* Politico (May 14, 2025), https://www.politico.com/news/2025/05/14/treasury-doge-disclosures-bank-stocks-00347972.

96. Tom Krause, the lead official for the DOGE-Treasury BFS team, has disclosed he owns hundreds of thousands of dollars' worth of shares in a wide range of financial companies, including those that provide services to the unit Krause oversees, such as Intuit, the parent company of Turbo Tax, a company that has lobbied heavily against IRS Direct File, a program Musk and DOGE have targeted for elimination.[32]

97. Notably, Krause remains employed with Cloud Software Group, which owns Citrix systems, an American multinational cloud computing and virtualization technology company that provides server, application and desktop virtualization, networking, software as a service (SAAS), and cloud computing technologies. Citrix products are used by approximately 99% of Fortune 100 companies and 98% of Fortune 500 companies.[33]

98. Additionally, DOGE-Treasury employees Todd Newnam and Linda Whitridge own shares of Intuit.

99. It is unclear whether Krause and the other DOGE-Treasury team members have been required to divest from any of their financial holdings. While Krause has disclosed a range of purchases and sales of assets, there have been no disclosures about any of his bank stock holdings.

---

[32] Michael Stratford, '*Glaring Red Flag': Treasury DOGE Team Discloses Bank Stock Holdings,* Politico (May 14, 2025), https://www.politico.com/news/2025/05/14/treasury-doge-disclosures-bank-stocks-00347972.

[33] During his earlier involvement with Citrix, Krause was brought in to reduce fraud in the company's practice, for which he implemented massive employee terminations and altered company IT systems for efficiency purposes. In connection with the changes Krause implemented at the company, Citrix experienced significant data breaches of highly sensitive information, prompting the Cybersecurity and Infrastructure Security Agency to designate two vulnerabilities in the Citrix software as the most exploited by hackers globally.

100. As stated in a recent Politico article about the glaring "red flags" of certain DOGE-Treasury employees, including Krause, Whitridge, and Newnam, "[a] person at this level of [the] Treasury Department should absolutely not have direct financial ties to the industries and the companies that he or she is in part responsible for overseeing."[34]

101. Julie Brinn Siegel, who was Treasury's deputy chief of staff during the Biden administration, sharply criticized the DOGE-Treasury team members' investments in tax preparation software maker Intuit, which has been lobbying against the IRS Direct File program. "The DOGE Team at Treasury killed free tax filing software, is outsourcing foundational technical infrastructure, and firing the cops who keep our financial system safe from catastrophe," she said. "They also have large holdings in the exact tax prep, government contracting and financial services companies that will profit from their actions. Who are they working for?"[35]

102. The Biden-era IRS Direct File program, which the Trump administration kept for this year, allows taxpayers to pay their taxes for free directly to the IRS rather than use costly private sector tax preparation software. According to public reporting, the administration plans to end the Direct File initiative, months after Musk reported that DOGE had "deleted" the government group working on it.[36]

103. Sam Corcos is a DOGE-Treasury employee serving as the Chief Information

---

[34] *Id.*

[35] *Id.*

[36] Fatima Hussein, *Trump administration plans to end the IRS Direct File Program for free tax tiling, AP Sources Say,* Associated Press (Apr. 17, 2025), https://apnews.com/article/irs-direct-file-tax-returns-free-trump-4bb0bca02fab9b3d06ae6f45ac67b7ab; Elon Musk (@elonmusk), X.com (Feb. 23, 2025, 14:35), https://x.com/elonmusk/status/1886498750052327520?s=46.

Officer at Treasury. Whereas his duties purportedly relate to planning, programming, budgeting, and executing decisions related to information technology ("IT") at Treasury, he has been reportedly responsible for organizing a "hackathon" within the IRS in order to implement a data system that integrates numerous data systems, potentially from across multiple other agencies' systems.[37]

b. DOGE's Cavalier Disregard for Information Security Spans Its Operations Across the Federal Government

104. DOGE's conduct outside of Treasury further demonstrates that DOGE, as a whole, cannot be trusted to faithfully follow the information security guidelines set out by Congress.

105. DOGE has sent teams of personnel to numerous federal departments and agencies, taken control of their computer systems, and even taken the lead in terminating numerous contracts and employees. *Does 1-26 v. Musk,* No. 25-cv-0462, 2025 WL 840574 (D. Md., Mar. 18, 2025). In January of 2025, after the DOGE Executive Order was signed, DOGE team members, including former private sector employees of Musk, arrived at the Office of Personnel Management ("OPM") and moved into the area of the office of the OPM Director, locking out senior career civil servants from the OPM computer systems. *Id*. at *5–6.

106. Such takeover conduct has been reported at numerous federal agencies, leading to numerous lawsuits.[38]

---

[37] Rebecca Heilweil, *DOGE Rep Sam Corcos Is Treasury's New Chief Information Officer, Source Says,* FedScoop (May 22, 2025), https://fedscoop.com/doge-sam-corcos-treasury-chief-information-officer/.

[38] *See*, *e.g.*, *Maryland v. Corporation for National and Community Service*, No. 25-cv-1363 (D. Md.); U.*S. Institute of Peace v. Jackson*, No. 25-cv-804 (D.D.C.); *ACLU v. U.S. Social Security Administration*, No. 25-cv-1217 (D.D.C.); *Aviel v. Gor*, No.25-cv-778 (D.D.C.); *American Counsel of Learned Societies v. McDonald*, 25-cv-3657 (S.D.N.Y.).

107. As of February 7, 2025, DOGE has been operating at the U.S. Departments of Education, Housing and Urban Development, Health and Human Services, Treasury, Transportation, Veteran Affairs, and Agriculture, as well as the National Oceanic and Atmospheric Administration; Federal Emergency Management Agency ("FEMA"); the Consumer Financial Protection Bureau; National Nuclear Security Administration; and the Centers for Medicare and Medicaid Services. *Id*. at *6, 8. Examples of DOGE's influence and impact on the various agencies include the following:

a. At the Department of Education, DOGE reportedly made almost all of the decisions about "what grants and contracts to cancel and which employees to put on leave, without seeking or considering input from political appointees;"[39]

b. The former Chief Financial Officer of FEMA submitted a declaration in the *Doe* litigation stating that, after observing DOGE conduct on February 10, 2025, the change in FEMA policy restricting sending certain resources to state and local governments, was a decision made by Musk or DOGE and not by FEMA (*Doe*, 2025 WL 840574, at *3); and

c. On January 24, 2025, after a directive from Secretary of State Marco Rubio directed a pause on new obligations of funding through the State Department and United States Agency for International Development ("USAID"), DOGE sought and eventually gained access to the U.S. Department of Treasury payment systems, including "root access" to USAID systems, which is the highest level of access. *Id.* at *4.

108. Since January 2025, DOGE has maintained a webpage containing a "wall of receipts" to publish the numerous federal contracts, federal dollars, and even jobs that have been

[39] Jeff Stein et al., *Musk's Blitzkrieg Is Unnerving Many of Trump's Senior Advisors,* The Washington Post (Feb. 21, 2025), https://www.washingtonpost.com/business/2025/02/21/doge-cuts-frustration-musk-trump/.

cut as a result of their efforts.[40] Public reporting has shown that it is riddled with errors.[41] Reporting has also revealed that an anonymous tech-group affiliated with 404Media hacked the DOGE website, due to a lack of security.[42]

109. In April, a whistleblower came forward to report unlawful access activity in data systems within the National Labor Relations Board ("NLRB").[43] According to the whistleblower, after DOGE employees were installed in the agency, IT observed numerous instances of unusual and suspicious activity, including impermissible data downloads, impermissible access into sensitive data sets, disabled security controls, and the creation of new user credentials. The whistleblower report further details a spike in IT access attempts from international credentials located in Russian territory, attempting to access sensitive NLRB data systems with the new user credentials that had been suspiciously and anonymously created. The whistleblower makes the connection that the NLRB's data breach stemmed from an internal actor.

110. Musk and his DOGE team have been reportedly working to create a massive database system "bridge"—or "mega API" (Application Programming Interface)—in order to create a software system that communicates across IRS databases and is intended to include

---

[40] Dep't of Govt. Efficiency (last updated May 11, 2025), https://doge.gov/savings.

[41] David A. Fahrenthold, *DOGE Removes Dozens of Resurrected Contracts From Its List of Savings,* The New York Times (May 13, 2025), https://www.nytimes.com/2025/05/13/us/politics/doge-musk-contracts-trump.html.

[42] James Bickerton, *Has Elon Musk's DOGE Website Been Hacked? What We Know,* Newsweek (Feb. 14, 2025), https://www.newsweek.com/elon-musk-doge-website-hacked-2031139.

[43] *See* Daniel Berulis, *Declaration* (Apr. 14, 2025), 2025_0414_Berulis-Disclosure-with-Exhibits.s.pdf

datasets of information from other federal agencies.[44] DOGE-Treasury employee Sam Corcos is purportedly spearheading the project, which involves working with third-party vendor Palantir. But "[s]eparation and segmentation is one of the core principles in sound cybersecurity."[45]

c. Harm to the States Caused by Defendants' Information Security Lapses

111. The States have suffered, and will continue to suffer, harm as a result of Defendants' disclosure of the States' Sensitive Data through expanded access granted to DOGE-Treasury team members, as well as significant cybersecurity lapses. These lapses have created a serious risk that the States' bank accounts and other financial information will be obtained and misused by bad actors.

112. Defendants' disregard for established information security requirements, as set out by Congress and NIST, have exposed the States' Sensitive Data to not only foreign interference but also insider threats from conflicted and inadequately vetted and trained DOGE employees.

4. Defendants' Change in Longstanding Policy Governing Disbursement of Federal Funds to the States

a. Treasury's Institutional Practice and Policy

113. The Administration's decision to implement a new payment request review process that pauses and potentially blocks disbursement of federal program funds based on ideology is a

[44] *See* Makena Kelly, *DOGE Is Planning a Hackathon at the IRS. It Wants Easier Access to Taxpayer Data,* WIRED (Apr. 5, 2025), https://www.wired.com/story/doge-hackathon-irs-data-palantir/; "Editor," *Palantir Assisting DOGE With Major Project for IRS,* Tech Business Daily (Apr. 12, 2025), https://techbusinessdaily.com/2025/04/12/palantir-assisting-doge-with-major-data-project-for-irs/

[45] Hannah Natanson et al., *DOGE Aims To Pool Federal Data, Putting Personal Information at Risk,* The Minnesota Star Tribune (May 8, 2025), https://www.startribune.com/doge-aims-to-pool-federal-data-putting-personal-information-at-risk/601347001.

fundamental problem: "it is not for the Treasury Department or the administration to decide which of our congressionally approved commitments to fulfill and which to cast aside."[46]

114. For decades, it was Treasury's practice and longstanding policy for BFS, when acting as "America's checkbook," to process the disbursement of funds in accordance with the coded data in the payment file as received from the submitting agency, with the submitting agency (and not BFS) bearing the responsibility of conducting a review of the propriety of the payment or eligibility of the payee except for screening through the "Do Not Pay" working system. In other words, "the agency responsible for making the payments always drives the payment process."[47]

115. BFS is a bureau traditionally managed by career civil servants. Importantly, the institutional practice and policy of Treasury is that BFS staff "do not independently determine a payment's eligibility" because that is the responsibility performed by the submitting agencies with respect to the specific laws and regulations governing their funding programs. Instead, the historic and longstanding practice and policy of Treasury in federal funding is to "ensure that requested payments are successfully and securely processed" by BFS through a limited, ministerial review.

116. As then-Secretary David Lebryk said in response to a request to grant Krause access to Treasury data systems in January, "I don't believe we have the legal authority to stop an

[46] Robert Rubin et al., *Five Former Treasury Secretaries: Our Democracy Is Under Siege*, The New York Times (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/opinion/treasure-secretaries-doge-musk.html.

[47] U.S. Dep't of Treas., *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), https://home.treasury.gov/news/press-releases/sb0009.

authorized payment certified by an agency,"[48] acknowledging Treasury's institutional practice and policy surrounding the disbursal of federal funds.

117. The "certifying officer" at the submitting agency who sends over the payment request "is responsible for … the legality of a proposed payment under the appropriation or fund involved," including adjudicating any payment flags that are raised by cross-checks with Do Not Pay databases. 31 U.S.C. § 3528(a). In contrast, BFS has no authority to directly alter requested payment amounts unless it is to "offset" (*i.e.*, redirect a portion of a payment toward) a known government debt, an authority provided in the Debt Collection Improvement Act of 1996. *See* Pub. L. 104-134, § 31001 (1996); *see also* 31 U.S.C. § 3716(c)(1)(A).

118. BFS's institutional policies protected the integrity of these federal payment systems and processes, ensuring insulation from political pressures or policy interests and focusing BFS's mission on reliability, accuracy, timeliness, operational efficiency, and privacy protections.

b. The DOGE-Treasury Engagement Plan

119. Musk has publicly posted that his DOGE-Treasury team, all dually appointed employees serving both DOGE and Treasury with access to BFS payment systems,[49] is "rapidly shutting down" payments to federal program fund recipients.[50]

120. At the President's direction, Treasury leadership developed a plan to engage a DOGE team to work at Treasury's BFS on a four-to-six-week project that would assist in

---

[48] *Id.*

[49] U.S. Dep't of Treas., *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), https://home.treasury.gov/news/press-releases/sb0009.

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

effectuating the President's Executive Orders to pause and block federal program funding that did not align with the President's priorities, contrary to congressional appropriation (the "Engagement Plan").

121. Under the Engagement Plan, the DOGE-Treasury team will create, and Treasury will implement, an automated process to pause and flag payment instructions for further review by the submitting agency under an ideological litmus test to determine if the payment aligns with the President's agenda and should be certified or blocked.

122. Pursuant to directives of the DOGE Executive Order, the DOGE-Treasury team initially prepared a four-to-six week plan by which it would create an automated process under the Engagement Plan to flag, pause, and revert to the submitting agency for selective cancellation payment requests in the BFS system. The Engagement Plan contemplated the use of BFS data pulled into a "sandbox" system in order to create a model to alter the IT systems currently in place at BFS such that the DOGE-Treasury team could effectuate the selection of particularly labeled payments, according to ideological criteria.

123. The Engagement Plan was developed by Defendants to "help operationalize the President's policy priorities ... by helping identify payments that may be improper under his new Executive Orders" and requires "pauses to certain types of financial transactions" that do not align with the President's policies. Krause Aff. ¶¶ 12, 17 (ECF No. 33). The plan called for embedding within BFS a DOGE team to develop an automated process for pausing and flagging payment files while in the BFS "landing zone" before certification by the submitting agency. The objective was to create an automated process that would flag payment files in the "pre-edit phase" for further review based on "certain Treasury Account Symbols" that would signal the payment was suspect, *i.e.*, may not align ideologically with the President's priorities and possibly should be blocked.

Treasury leadership had begun "operationalizing" the Engagement Plan as soon as Krause was brought on board at Treasury on January 23, 2025.

124. The Engagement Plan was already in its "initial stages" of implementation when the Court issued the TRO in this case. Elez had already been given "access to and was analyzing copies of the source code for certain BFS payment systems" on his Treasury laptop. Accordingly, the Engagement Plan reflected Treasury's final decision on how to carry out the President's Executive Orders—a decision that culminated in the operationalization of the Engagement Plan on January 23, 2025.

c. Harm to the States Caused by Defendants' Change in Treasury's Historic and Longstanding Practice and Policy for Reviewing Funding Requests

i. BFS Reimbursements to States

125. BFS disburses billions of dollars every year directly to the States through a host of federal programs that are critical for the States to provide vital services for their residents.

126. For the States to receive their billions of dollars in federal funds, they operate, in many instances, on a reimbursement model. The State pays from its treasury for State-administered federal programs, and on the back end seeks federal reimbursement through the federal government's funding portal system. In those instances where federal reimbursement is sent by wire, sensitive State wiring and ACH bank account information is provided in order for the funds to be directed to the State.

127. Federal programs administered by, for example, FEMA, the Department of Energy, the Environmental Protection Agency, the Federal Highway Administration, and Health and Human Services operate on a reimbursement model.

128. For example, Plaintiffs collectively were awarded approximately $1.9 billion in federal funds under the Solar for All program administered by the EPA.[51] That program is administered on a reimbursement model, where each State recipient first incurs actual costs and then seeks reimbursement from EPA.

129. As another example, many of the States participate in the Foster Care Program administered by HHS's Office of the Administration for Children and Family Services. That program provides reimbursements for actual costs incurred by the States in administering a program for foster care services that has been approved by the federal government. *See* 42 U.S.C. § 674.

130. The current Administration has already made numerous efforts to unlawfully execute President Trump's defunding executive orders.[52] The Engagement Plan is simply another tactic deployed to achieve the same ends, but just through the agency that disburses the funds, rather than through the agencies that submit the disbursement requests.

131. The States have a strong interest in ensuring that they continue to receive timely reimbursement under these critical federal programs despite the current Administration's ideological preferences. Any delay or potential halt of reimbursement to the States for the billions

[51] U.S. Environmental Protection Agency, *Solar for All* (updated May 19, 2025), https://www.epa.gov/greenhouse-gas-reduction-fund/solar-all.

[52] *See*, *e.g.*, *New York v. Trump*, No. 25-cv-39, 2025 WL 715621 (D.R.I. Mar. 6, 2025) (holding that agencies' implementation of executive order categorically freezing funds likely violated APA and the Constitution); *Washington v. Trump*, No. 25-cv-00244, 2025 WL 659057 (D. Wash. Feb. 28, 2025) (holding that agency implementation of executive order denying funding if recipients fail to comply with President's executive order likely violated APA and the Constitution); *Maine v. U.S. Dep't of Agriculture*, 2025 WL 1088946 (D. Me. Apr. 11, 2025) (holding that agency's declaration that Maine Department of Education was in violation of Title IX—following President Trump's executive order purporting to interpret Title IX—likely violated the APA).

of dollars they front to their residents under these federal programs will cause material and substantial financial harm to the States, including the cost the States would be forced to incur to provide additional services to residents who are denied these federal benefits to ensure the continued welfare of their residents.

ii. Treasury Offset Program

132. The Treasury Offset Program ("TOP") is also operated by Treasury through BFS. This automated and centralized program intercepts both federal and state payments (for participating reciprocal States, as explained below) to satisfy debts owed to federal or state agencies. Depending on the nature of the debt and the federal source from which it is withheld, offsets range from 15% to 100%.[53]

133. States are often recipients of offset funds, *i.e*. they are often the creditors to whom money is owed. This occurs when debtors owe state taxes, child support, SNAP debt, and unemployment debt, to name some examples. Through TOP, states recovered $720.9 million in state income tax debt in fiscal year 2024.[54] They also recovered $197.9 million in delinquent SNAP debt, in addition to $343.7 million in debts related to state unemployment insurance (arising from fraud or failure to report earnings, on the one hand, and unpaid employer unemployment tax debt, on the other).[55]

---

[53] U.S. Dep't of the Treas., Bur. of Fisc. Serv., *Treasury Offset Program Fact Sheet*, (last visited May 23, 2025), https://fiscal.treasury.gov/files/top/TOP-rules-reqs-fact-sheet.pdf.

[54] U.S. Dep't of the Treas., Bur. of the Fisc. Serv., *Treasury Offset Program (TOP), How the Treasury Offset Program Collects Money for State Agencies* (last visited May 23, 2025), https://www.fiscal.treasury.gov/top/state-programs.html.

[55] *Id.*

134. Some States enter into an agreement whereby TOP offsets federal non-tax payments against other debts owed to state agencies. In return, those States offset their own payments for delinquent debt owed to the federal government. This is known as the State Reciprocal Program. States participating in this program recovered $76.2 million in fiscal year 2024.[56]

135. In fiscal year 2024, TOP recovered $1.4 billion in child support obligations. These payments benefit the recipients, but also the States where those recipients reside. Those States enjoy a widened tax base and might be subject to reduced entitlement claims by those families. Additionally, the States may themselves receive money from those child-support offsets. For example, the Temporary Assistance for Needy Families ("TANF") program requires families receiving assistance to assign their right to child support to the State. 42 U.S.C. § 608(a)(3); *see, e.g.*, Ariz. Rev. Stat. § 46-407(A) (assigning support rights to the State where the parent entitled to the support has benefited from TANF); N.Y. Comp. Codes R. & Regs. tit. 18, § 369.1 (same). Therefore, a child support obligation that goes unfulfilled is often a monetary harm to the state.

136. To facilitate child support offsets, States report to Treasury those individuals who owe child support to state residents. In response, Treasury diverts payments (primarily but not exclusively federal tax refunds) meant for those debtors, to the state agency responsible for child support. That agency then distributes the money to the recipients (or assignees).

137. The Engagement Plan puts the States at imminent risk of delays in receiving these critically important offsets for child support payments to their residents.

[56] *Id.*

CAUSES OF ACTION

COUNT ONE
Violation of APA § 706(2)(A) – Arbitrary and Capricious
Against Treasury and Secretary Bessent

138. The States reallege and incorporate by reference the allegations set forth in the preceding paragraphs.

139. The APA provides that courts must "hold unlawful and set aside" agency action that is "arbitrary, capricious, [or] an abuse of discretion." 5 U.S.C. § 706(2)(A).

140. By failing to protect the States' Sensitive Data, including by permitting DOGE-Treasury employees to access the Sensitive Data without adequate vetting or training; by failing to prevent DOGE-Treasury employees from sharing sensitive data outside of Treasury; and by failing to account for insider threats and adequately respond to them, Treasury and Secretary Bessent ("Agency Defendants") have acted arbitrarily and capriciously, exposing the States to significant cybersecurity risks ("Access Agency Action").

141. Furthermore, where the agency changes its position, the agency's conduct is arbitrary and capricious unless the agency "provide[s] a reasoned explanation for the change," "display[s] awareness that [it is] changing position," and considers "serious reliance interests." *Encino Motorcars, LLC v. Navarro*, 579 U. S. 211, 221–22 (2016) (quoting *FCC v. Fox Television Stations, Inc*., 556 U. S. 502, 515 (2009)). These requirements—applicable under the Supreme Court's "change-in-position doctrine"—are to ensure that an agency does "not mislead regulated entities." *Food & Drug Admin. v. Wages and White Lion Investments, L.L.C*., 604 U.S. ___, 2025 WL 978101, at *13 (April 2, 2025).

142. An agency changes its position when it acts inconsistently with an earlier position, performs a reversal of its former views as to the proper course, or disavows prior inconsistent agency action as no longer appropriate. *Id*. at *14.

143. Agency Defendants' implementation of the Engagement Plan is arbitrary and capricious because Defendants have failed to provide a reasoned explanation for the change from longstanding Treasury policy and practice to expand BFS's limited, ministerial role in processing payment requests already approved by the submitting federal agency to pause and potentially block payments on ideological grounds.

144. Agency Defendants' implementation of the Engagement Plan is also arbitrary and capricious because Defendants have failed to consider the States' significant reliance interests in the prompt and timely processing of their reimbursement requests under BFS's longstanding limited, ministerial review procedure and the harms that flow to the States from the new automated review process under the Engagement Plan that will flag, pause, and potentially block payments on ideological grounds.

145. Agency Defendants have therefore acted in a manner that is "arbitrary, capricious, [or] an abuse of discretion" in violation of the APA. 5 U.S.C. § 706(2)(A).

146. Agency Defendants' violation causes ongoing harm to Plaintiffs.

147. The States are further entitled to a permanent injunction against the Agency Defendants from engaging in the Access Agency Action and implementing the Engagement Plan.

COUNT TWO
Violation of APA § 706(2)(A) – Contrary to Law
Against Treasury and Secretary Bessent

148. The States reallege and incorporate by reference the allegations set forth in the preceding paragraphs.

149. Under the APA, a court must set "aside agency action" that is "not in accordance with law." 5 U.S.C. § 706(2)(A).

150. Under FISMA, Treasury is required to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. Treasury was further required to comply with standards implementing FISMA set out by NIST. 44 USC §§ 3543-3545.

151. By failing to protect the States' Sensitive Data, including by permitting DOGE-Treasury employees to access the Sensitive Data without adequate vetting or training; by failing to prevent DOGE-Treasury employees from sharing sensitive data outside of Treasury; and by failing to account for insider threats and adequately respond to them, Agency Defendants have failed to comply with numerous NIST requirements including, but not limited to, requirements governing access controls, information exchange, insider threats, and personnel sanctions.

152. Additionally, Title 18 of the U.S. Code imposes ethics rules on federal employee conduct in order to avoid conflicts of interest, including those that arise from personal interests that affect official action. *See* 18 U.S.C. § 208(a); *see also* 5 C.F.R. part 260. SGEs are governed by these ethics rules, including § 208(a), and are subject to penalties under section 216 of the Code. *See* 18 U.S.C. § 216 (describing the penalties and injunctions for violating, *inter alia*, §§207 and 208, which include civil penalties up to $50,000 for each violation, or an injunction to enjoin further violations). The only exception from § 208(a)'s requirements relevant here would be for the appointing official of an SGE (with a duly filed financial disclosure pursuant to chapter 5 of title 31) to review the SGE's disclosure and certify that the SGE's work "outweighs the conflict

of interest." 18 U.S.C. § 207(c). The statute does not authorize disclosure to an SGE without such a certification.

153. Furthermore, the Engagement Plan was put in place by the Agency Defendants in contravention of duly enacted statutes appropriating funds to the States, to be disbursed by Treasury.

154. Agency Defendants have failed to comply with the dictates of each of these statutes and regulations.

155. Agency Defendants' violations cause ongoing harm to States and their residents.

156. The States are further entitled to a permanent injunction against the Agency Defendants from engaging in the Access Agency Action and implementing the Engagement Plan.

COUNT THREE
Violation of the Separation of Powers Doctrine—Usurping Legislative Authority
Against All Defendants

157. The States reallege and incorporate by reference the allegations set forth in the preceding paragraphs.

158. Article I, Section 1 of the United States Constitution enumerates that: "[a]ll legislative Powers herein granted shall be vested in Congress." U.S. Const. art. I, sec. 1. "The Framers viewed the legislative power as a special threat to individual liberty, so they divided that power to ensure that 'differences of opinion' and the 'jarrings of parties' would 'promote deliberation and circumspection' and 'check excesses in the majority.'" *Seila Law LLC v. CFPB*, 591 U.S. 197, 223 (2020) (quoting The Federalist No. 70, at 475 (A. Hamilton) and No. 51, at 350)).

159. "As Chief Justice Marshall put it, this means that 'important subjects … must be entirely regulated by the legislature itself,' even if Congress may leave the Executive 'to act under

such general provisions to fill up the details.'" *West Virginia v. EPA*, 597 U.S. 697, 737 (2022) (Gorsuch, J., concurring) (quoting *Wayman v. Southard*, 10 Wheat. 1, 42–43, 6 L.Ed. 253 (1825)).

160. The Separation of Powers doctrine thus represents a central tenet of our Constitution. *See, e.g., Trump v. United States*, 603 U.S. 593, 637–38 (2024); *Seila Law LLC*, 591 U.S. at 227.

161. Consistent with these principles, Executive Branch powers are limited to those specifically conferred by the Constitution and federal statutes, and do not include any undefined residual or inherent power.

162. The United States Constitution does not authorize the Executive Branch to enact, amend, or repeal statutes. *Clinton v. City of New York*, 524 U.S. 417, 438 (1998).

163. Indeed, Executive Branch officials act at the lowest ebb of their constitutional authority and power when they act contrary to the express or implied will of Congress. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

164. Executive Branch agencies derive their rulemaking authority from statutes enacted by Congress, which prescribe the manner in which agencies are to regulate.

165. Where the President, by Executive Order or otherwise, directs an agency to take an action that runs afoul of a statute or the legislative intent of Congress, such action violates the Separation of Powers doctrine.

166. Here, Defendants have acknowledged that the purpose of the Engagement Plan is to enable Treasury to pause and block payments to States and their residents of federal funds that have been appropriated by Congress based on ideological grounds.

167. The clear objective of the Engagement Plan is to usurp Congress's power of the purse in violation of the Separation of Powers doctrine.

168. For the same reasons that the Engagement Plan exceeds statutory authority, it also usurps Congress's exclusive legislative authority and contravenes its express statutory mandates restricting the disclosure of private information by federal agencies. *See Clinton*, 524 U.S. at 438; *see also* 5 U.C.S. § 552a(b).

169. This Court is authorized to enjoin any action by the Executive Branch that "is unauthorized by statute, exceeds the scope of constitutional authority, or is pursuant to unconstitutional enactment." *Youngstown Sheet & Tube Co. v. Sawyer*, 103 F. Supp. 569 (D.D.C. 1952), aff'd, 343 U.S. 579 (1952).

170. The States are further entitled to a permanent injunction against the Agency Defendants from implementing the Engagement Plan.

COUNT FOUR
Violation of the Take Care Clause
Against All Defendants

171. The States reallege and incorporate by reference the allegations set forth in the preceding paragraphs.

172. The Take Care Clause provides that the President must "take Care that the Laws be faithfully executed …." U.S. Const. art. II, sec. 3, cl. 3; *UARG v. EPA*, 573 U.S. 302, 327 (2014) ("Under our system of government, Congress makes the laws and the President … faithfully executes them.").

173. In many instances, Congress has delegated to federal agencies the authority to implement laws through regulation.

174. "Withholding congressionally appropriated funds … simply cannot be construed as following through on [the] constitutional mandate" set forth in the Take Care Clause. *Widakuswara v. Lake*, No. 25-cv-2390, 2025 WL 945869, at *7 (S.D.N.Y. Mar. 28, 2025).

175. By directing that the Engagement Plan be adopted and implemented, the President has failed to faithfully execute the laws enacted by Congress in violation of the Take Care Clause.

176. Pursuant to 28 U.S.C. § 2201, the States are entitled to a declaration that the Engagement Plan violates the Take Care Clause of the U.S. Constitution.

177. The States are further entitled to a permanent injunction against the Agency Defendants from implementing the Engagement Plan.

PRAYER FOR RELIEF

WHEREFORE, the States pray that this Court:

a. Issue a permanent injunction barring Agency Defendants from granting access to Treasury payments or any other data systems maintained by Treasury 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 information security training called for in federal statutes and Treasury regulations, and otherwise complied with all requirements of the Federal Information Security Modernization Act; and otherwise excluding from the scope of the injunction access by political appointees, contractors on the approved outside contractor list maintained by Treasury's Chief Information Officer as necessary to perform routine or emergency maintenance on BFS systems, or the Federal Reserve Bank of Kansas City;

b. Issue a permanent injunction barring Agency Defendants from implementing a new process for reviewing federal funding payment request for the purpose of pausing and potentially blocking disbursement of funds based on ideological criteria;

c. Issue a declaration that it is unlawful for Defendants to grant access to Treasury payments or any other data systems maintained by Treasury 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 information security training called for in federal statutes and Treasury regulations, and otherwise failed to comply with the requirements of the Federal Information Security Modernization Act, excluding political appointees, contractors on the approved outside contractor list maintained by Treasury's Chief Information Officer as necessary to perform routine or emergency maintenance on BFS systems, or the Federal Reserve Bank of Kansas City;

d. Issue a declaration that altering the Treasury policy for reviewing federal funding payment requests received by BFS in order to selectively pause and potentially

block appropriated federal funding based on ideological grounds is unlawful and unconstitutional;

e. Award the States their reasonable fees, costs, and expenses, including attorneys' fees, pursuant to 28 U.S.C. § 2412; and

f. Award such other relief as this Court may deem just and proper.

Dated: New York, New York
May 23, 2025

LETITIA JAMES
ATTORNEY GENERAL OF NEW YORK

By: */s Andrew Amer*
Andrew Amer
Special Counsel
Rabia Muqaddam
Special Counsel for Federal Initiatives
Colleen K. Faherty
Special Trial Counsel
Stephen C. Thompson
Special Counsel
28 Liberty Street
New York, NY 10005
(212) 416-6127
andrew.amer@ag.ny.gov

Counsel for the State of New York

KRISTEN K. MAYES
ATTORNEY GENERAL OF ARIZONA

By: */s Joshua D. Bendor*
Joshua D. Bendor
Joshua A. Katz
2005 North Central Avenue
Phoenix, Arizona 85004
(602) 542-3333
Joshua.Bendor@azag.gov
Joshua.Katz@azag.gov

Counsel for the State of Arizona

ROB BONTA
ATTORNEY GENERAL OF CALIFORNIA

By: /s/ *Michael S. Cohen*
Michael S. Cohen
Deputy Attorney General
Thomas S. Patterson
Senior Assistant Attorney General
Mark R. Beckington
John D. Echeverria
Supervising Deputy Attorneys General
Nicholas Green
Jay Russell
Deputy Attorneys General
California Attorney General's Office
1300 I Street, Suite 125
P.O. Box 944255
Sacramento, CA 94244-2550
(916) 210-6090
Michael.Cohen@doj.ca.gov

Counsel for the State of California

PHIL WEISER
ATTORNEY GENERAL OF COLORADO

By: */s Shannon Stevenson*
Shannon Stevenson
Solicitor General
Office of the Colorado Attorney General
1300 Broadway, #10
Denver, CO 80203
(720) 508-6000
shannon.stevenson@coag.gov

Counsel for the State of Colorado

WILLIAM TONG
ATTORNEY GENERAL OF CONNECTICUT

By: */s Matthew Fitzsimmons*
Matthew Fitzsimmons
Chief Counsel
165 Capitol Ave
Hartford, CT 06106
(860) 808-5318
Matthew.fitzsimmons@ct.gov

Counsel for the State of Connecticut

KATHLEEN JENNINGS
ATTORNEY GENERAL OF THE STATE OF DELAWARE

By: /s/ *Vanessa L. Kassab*
Vanessa L. Kassab
Deputy Attorney General
Delaware Department of Justice
820 N. French Street
Wilmington, DE 19801
(302) 683-8899
vanessa.kassab@delaware.gov

Counsel for the State of Delaware

ANNE E. LOPEZ
ATTORNEY GENERAL OF HAWAI'I

By: /s *Kaliko'onālani D. Fernandes*
David D. Day
Special Assistant to the Attorney General
Kaliko'onālani D. Fernandes
Solicitor General
425 Queen Street
Honolulu, HI 96813
(808) 586-1360
kaliko.d.fernandes@hawaii.gov

Counsel for the State of Hawai'i

KWAME RAOUL
ATTORNEY GENERAL OF ILLINOIS

By: */s/ Darren Kinkead*
Darren Kinkead
Public Interest Counsel
115 S. LaSalle St.
Chicago, Illinois 60603
(773) 590-6967
Darren.Kinkead@ilag.gov

Counsel for the State of Illinois

AARON M. FREY
ATTORNEY GENERAL OF MAINE

By: /s/ *Jason Anton*
Jason Anton
Assistant Attorney General
Office of the Attorney General
6 State House Station
Augusta, ME 04333-0006
(207) 626-8800
jason.anton@maine.gov

Counsel for the State of Maine

ANTHONY G. BROWN
ATTORNEY GENERAL OF MARYLAND

By: /s *Adam D. Kirschner*
Adam D. Kirschner
Senior Assistant Attorney General
Office of the Attorney General
200 Saint Paul Place, 20th Floor
Baltimore, Maryland 21202
(410) 576-6424
akirschner@oag.state.md.us

Counsel for the State of Maryland

ANDREA JOY CAMPBELL
ATTORNEY GENERAL
COMMONWEALTH OF MASSACHUSETTS

By: /s/ David C. Kravitz
David C. Kravitz
State Solicitor
One Ashburton Place
Boston, MA 02108
617-963-2427
david.kravitz@mass.gov

Counsel for the Commonwealth of Massachusetts

KEITH ELLISON
ATTORNEY GENERAL OF MINNESOTA

By: /s *Liz Kramer*
Liz Kramer
Solicitor General
445 Minnesota Street, Suite 1400
St. Paul, Minnesota, 55101
(651) 757-1010
Liz.Kramer@ag.state.mn.us

Counsel for the State of Minnesota

AARON D. FORD
ATTORNEY GENERAL OF NEVADA

By: /s/ *Heidi Parry Stern*
Heidi Parry Stern (Bar. No. 8873)
Solicitor General
Office of the Nevada Attorney General
1 State of Nevada Way, Suite 100
Las Vegas, NV 89119
HStern@ag.nv.gov

Counsel for the State of Nevada

MATTHEW J. PLATKIN
ATTORNEY GENERAL OF NEW JERSEY

By: */s David Leit*
David Leit
Assistant Attorney General
(609) 414-4301
david.leit@law.njoag.gov

Kashif Chand
Chief, Deputy Attorney General
(609) 696-5160
kashif.chand@law.njoag.gov
124 Halsey Street
Newark, NJ 07101

Counsel for the State of New Jersey

JEFF JACKSON
ATTORNEY GENERAL OF NORTH CAROLINA

LAURA HOWARD
CHIEF DEPUTY ATTORNEY GENERAL

By /s/ Daniel P. Mosteller
Associate Deputy Attorney General
North Carolina Department of Justice
PO Box 629
Raleigh, NC 27602
919-716-6026
dmosteller@ncdoj.gov

Counsel for State of North Carolina

DAN RAYFIELD
ATTORNEY GENERAL OF OREGON

By: */s/ Elleanor H. Chin*
Elleanor H. Chin
Senior Assistant Attorney General
Department of Justice
100 SW Market Street
Portland, OR 97201
(971) 673-1880
elleanor.chin@doj.oregon.gov

Counsel for the State of Oregon

PETER F. NERONHA
ATTORNEY GENERAL OF RHODE ISLAND

By: /s/ Alex Carnevale
Alex Carnevale
Special Assistant Attorney General
Office of the Attorney General – State of Rhode Island
150 South Main Street
Providence, RI 02903
(401) 274 4400
acarnevale@riag.ri.gov

Counsel for the State of Rhode Island

JOSH KAUL
ATTORNEY GENERAL OF WISCONSIN

By: */s/ Brian P. Keenan*
Brian P. Keenan
State Bar #1056525
Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 266-0020
keenanbp@doj.state.wi.us

Counsel for the State of Wisconsin

CHARITY R. CLARK
ATTORNEY GENERAL OF VERMONT

By: */s/ Jonathan Rose*
Jonathan Rose
Solicitor General
Appellate Unit
Office of the Attorney General
109 State Street, 3rd Floor
Montpelier, VT 05609
(802) 793-1646
jonathan.rose@vermont.gov

Counsel for the State of Vermont