

IN THE UNITED STATES DISTRICT COURT
 FOR THE EASTERN DISTRICT OF VIRGINIA
 Alexandria Division

ELECTRONIC PRIVACY)
 INFORMATION CENTER, *et al.*,)
)
 Plaintiffs,)
)
 v.)
)
 U.S. OFFICE OF PERSONAL)
 MANAGEMENT, *et al.*,)
)
 Defendants.)

Case No. 1:25-cv-255 (RDA/WBP)

MEMORANDUM OPINION AND ORDER

This matter comes before the Court upon Plaintiffs’ Motion for Temporary Restraining Order (“TRO”) (“Motion”). Dkt. 5. Given “the fluidity of the relationship between TROs and preliminary injunctions” and that “the opposing party [has] had a fair opportunity to oppose it,” the Court will consider Plaintiffs’ Motion for a TRO as one for a preliminary injunction.¹ *U.S. Dep’t of Lab. v. Wolf Run Mining Co.*, 452 F.3d 275, 283 (4th Cir. 2006) (“[T]he district court could properly consider a motion for a TRO as a request for a preliminary injunction, based on the fluidity of the relationship between TROs and preliminary injunctions, focusing not on a specific time period but on whether the opposing party had a fair opportunity to oppose it.”). Considering the Motion and accompanying exhibits and declarations, together with Plaintiffs’ Memorandum

¹ Defendants have requested that the Court convert Plaintiffs’ Motion into one for preliminary injunction because “Defendants have ‘had a fair opportunity to oppose it.’” Dkt. 19 at 1 n.1 (quoting *Wolf Run Mining Co.*, 452 F.3d at 283); *see also Sci. Sys. & Applications, Inc. v. United States*, 2014 WL 3672908, at *3 (D. Md. July 22, 2014) (explaining that “a district court can consider a motion for a TRO as a request for a preliminary injunction, so long as the opposing party was given notice sufficient to allow for a fair opportunity to oppose it.”); *Flora v. Mountain Valley Pipeline, LLC*, 2018 WL 3715761, at *1 (W.D. Va. Aug. 3, 2018) (“Because MVP was given notice and an opportunity to oppose the motion, the court will treat it as one for preliminary injunction.”).

in Support, Dkt. 7, Defendants' Memorandum in Opposition, Dkt. 19, Plaintiffs' Reply, Dkt. 20, and the argument heard during the February 21, 2025 hearing,² this Court DENIES Plaintiffs' Motion for the reasons that follow.

I. BACKGROUND

A. Factual Background

Plaintiffs Doe 1 and Electronic Privacy Information Center ("EPIC") (collectively, "Plaintiffs") bring a five-count Complaint against the U.S. Office of Personal Management ("OPM"), Charles Ezell in his official capacity as Acting Director of OPM, the U.S. Department of Treasury ("Treasury"), and Scott Bessent, Secretary of the Treasury (collectively, the "Government Defendants"), as well as the U.S. DOGE Service ("USDS" or "DOGE"); the Acting U.S. DOGE Administrator; and the U.S. DOGE Service Temporary Organization (collectively, the "DOGE Defendants"), alleging that Defendants have orchestrated "the largest and most consequential data breach in U.S. history." Dkt. 1 ¶¶ 1-3. Plaintiff Doe 1 is a current federal employee of an unnamed federal agency, and Plaintiff EPIC is a nonprofit organization suing on behalf of its members. *Id.* ¶¶ 9-10.

On January 20, 2025, President Donald J. Trump signed Executive Order 14158, Establishing and Implementing the President's "Department of Government Efficiency" (the "Executive Order"). *Id.* ¶ 32; Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025). In addition to recognizing and renaming the U.S. Digital Service as the U.S. DOGE Service, the Executive Order also established the role of U.S. DOGE Service Administrator and created the

² The Court acknowledges and appreciates counsel for both Plaintiffs and Defendants in the ethics and professionalism that they have exhibited thus far; particularly, in correcting attestations and the candor which was demonstrated with regard to certain developments in the case. The Court also notes that the parties' positions were exceptionally argued during the February 21, 2025 hearing.

U.S. DOGE Service Temporary Organization. Dkt. 1 ¶¶ 33-34. The Executive Order also required each Agency Head to establish a “DOGE Team” consisting of four employees within their respective agencies. *Id.* ¶ 35. Each DOGE Team would “coordinate their work with USDS and advise their respective Agency Heads on implementing the President’s DOGE Agenda.” *Id.* The Executive Order further instructed the U.S. DOGE Administrator to “commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems,” working with Agency Heads to “promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.” *Id.* ¶ 36. To accomplish this initiative, the Executive Order required Agency Heads “to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems.” *Id.* ¶ 37. Finally, the Executive Order directed USDS to adhere to “rigorous data protection standards,” *id.*, and stated that the “order shall be implemented consistent with applicable law,” Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025).

Plaintiffs allege that, since February 20, 2025, USDS personnel have obtained unprecedented access to information systems across numerous federal agencies, including Treasury and OPM. *Id.* ¶ 38. In this regard, Treasury operates the Bureau of Fiscal Service (“BFS”), which manages “a federal payment system that distributes nearly 90% of all federal payments, including Social Security benefits, tax refunds, and vendor payments.” *Id.* ¶ 42. The BFS payment systems contain the sensitive personal data, such as full Social Security numbers, of “tens of millions of individuals.” *Id.* ¶¶ 43, 45. OPM manages the Enterprise Human Resources Integration (“EHRI”) system, which is “responsible for maintaining the integrity of the electronic Official Personnel Folder (eOPF), which protects information rights, benefits, and entitlements of

federal employees.” *Id.* ¶ 77. The EHRI contains “Social Security numbers, dates of birth, salaries, home addresses, and job descriptions of all civil government workers, along with any disciplinary actions they have faced.” *Id.* ¶ 80. Plaintiffs further assert that the BFS and EHRI systems and the information contained therein are typically protected by information security protocols mandated by the Federal Information Security Act of 2014 (“FISMA”), privacy protections established by the Privacy Act of 1974 (the “Privacy Act”), and supervision by trained personnel. *Id.* ¶¶ 39, 46, 81-83.

Plaintiffs allege that, at the direction of the DOGE Defendants, the Government Defendants have abandoned these safeguards by providing the DOGE Defendants with unlawful access to sensitive and protected data in the BFS and EHRI systems and allowing the data to be used for prohibited purposes. *Id.* ¶¶ 49-76, 84-95.

On January 27, 2025, after being confirmed as Secretary of the Treasury, Defendant Scott Bessent granted USDS personnel access to the BFS payment systems, allegedly giving USDS personnel the ability to “stop payments from the federal government.” *Id.* ¶¶ 55, 56. As a consequence of granting this access, Plaintiffs assert that Secretary Bessent and the Treasury Department disclosed personal information contained in those systems to individuals not authorized by law to access them. *Id.* ¶ 57. After USDS personnel received access to the BFS systems, the official USDS/DOGE account on Twitter/X tweeted that it was “stopping improper payments.” *Id.* ¶ 69. Similarly, Elon Musk, “an individual who is either Acting USDS Administrator or otherwise exercising substantial authority within USDS,” *id.* ¶ 31, stated on his personal Twitter/X account that “[t]he @DOGE team is rapidly shutting down these illegal payments.” *Id.* ¶ 68. Plaintiffs further allege that, upon information and belief, USDS and Treasury personnel are unlawfully exfiltrating identifying information from the BFS payment

systems and redisclosing the information to individuals not employed at Treasury, *id.* ¶¶ 70-74, and that USDS is moving to “stop approved payments to federal contractors, charities that provide social services, and other federal departments,” *id.* ¶ 76.

On January 20, 2025, Plaintiffs allege that Musk and USDS personnel entered OPM’s headquarters and took control of the computer systems. *Id.* ¶¶ 85-86. According to Plaintiffs, at least six USDS agents were given “broad access to all personnel systems, including the EHRI system,” giving them the ability to access databases that “store medical histories, personally identifiable information, workplace evaluations, and other private data.” *Id.* ¶¶ 86-87.

Plaintiffs further allege that, on information and belief, the USDS personnel who have access to Treasury and OPM systems “lack training in applicable security safeguards for personal information, do not have relevant Treasury or OPM experience, may not have necessary security clearances, and may not be federal employees.” *Id.* ¶ 91.³ As such, Plaintiffs contend that the Government Defendants’ grant of systems access to the DOGE Defendants constitutes unlawful disclosure of personal data—including social security numbers and tax information—belonging to tens of millions of people stored in the BFS systems and the unlawful disclosure of personal data belonging to millions of federal employees stored in the EHRI system. Dkt 7 at 4-5.

As an “alternative” theory of complaint, Plaintiff Doe 1 alleges that, as a career civil servant, OPM retains her personal information on EHRI, including her Social Security number, home address, and disciplinary record. *Id.* Plaintiffs also allege that Doe 1 and many of EPIC’s

³ During the February 21, 2025 hearing, Counsel for Defendants was unable to provide a specific statement as to the level of training that the individuals on the DOGE Teams within Treasury and OPM received prior to receiving access to the information systems. To be sure, while the possible lack of training causes the Court some concern given the vast amounts of data contained in these systems, it does not impact, at this time, the appropriateness of injunctive relief based on the record before the Court.

members have filed federal tax returns electronically within the last six years. *Id.* As a result, the BFS systems contain extensive financial information about them, including statutorily protected return information. *Id.* Plaintiffs therefore assert that their “sensitive, confidential, and personally identifiable information has been unlawfully accessed and endangered by DOGE.” Dkt. 7 at 1. Plaintiffs further assert “[b]eyond the immediate harm of disclosure, Plaintiffs face substantially elevated risk of: data errors which could interfere with their paychecks or other employment benefits, purposeful withholding of payments to which they are legally entitled, and identity theft.” Dkt. 7 at 14.

The Court notes that Defendants dispute the claim that USDS personnel have obtained access to these information systems. Dkt. 19 at 1-2. Instead, Defendants assert that

In response to lawful Executive Orders issued by President Trump, Treasury and OPM have assembled teams of the agencies’ own employees, including detailees, to oversee implementation of the new Administration’s policies to root out waste, fraud, and abuse across the federal government. Although these teams liaise with USDS—a component of the Executive Office of the President—it is the agencies’ employees, and only those employees, who have access to the data systems containing the personal information upon which Plaintiffs premise their claims.

Id. Defendants therefore contend that Plaintiffs’ claims of unlawful access to the information systems by USDS personnel cannot be correct. *Id.* at 2.

B. Procedural Background

On February 10, 2025, Plaintiffs filed a Complaint in this Court, alleging five Counts against Defendants for the alleged misconduct. Dkt. 1. Plaintiffs filed the instant Motion for injunctive relief and a Memorandum in Support on February 12, 2025. Dkts. 5; 7. On February 14, 2025, the parties filed a Joint Motion to Set Briefing Schedule and Hearing regarding the Motion for injunctive relief, and the Court granted the Joint Motion, setting a briefing schedule and a hearing for February 21, 2025. Dkt. 9. On February 17, 2025, Plaintiffs submitted a Notice

of Factual Development, correcting allegations made in the Complaint and in support of their Motion. Dkt. 18. Defendants filed their Memorandum in Opposition on February 18, 2025, and Plaintiffs filed their Reply on February 19, 2025. Dkts. 19; 20. Defendants also submitted a Notice withdrawing n.6 of their Memorandum in Opposition on February 19, 2025. Dkt. 21. A hearing regarding the Motion for injunctive relief was held before this Court on February 21, 2025. Dkt. 32. Following the hearing, Plaintiffs submitted a Notice of Supplemental Authority informing the Court of additional cases that they discovered after the hearing. Dkt. 33.

Ultimately, with their request for injunctive relief, Plaintiffs seek an order:

“(1) enjoining the Department of Treasury (“Treasury”) and Office of Personnel Management (“OPM”) from allowing DOGE-affiliated personnel to access Bureau of Fiscal Services or Enterprise Human Resources Integration systems; (2) enjoining DOGE-affiliated personnel from accessing Treasury or OPM systems containing personally identifiable information except consistent with relevant SORNs; and (3) requiring Defendants Treasury and OPM to file a status report within 24 hours of the issuance of a Temporary Restraining Order, confirming that DOGE-affiliated personnel no longer have access to EHRI or BFS systems.”

Dkt. 5 at 1.

II. STANDARDS OF REVIEW

A. Standing

Article III standing requires a plaintiff to have “(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992)). An organization suing on behalf of its members must satisfy three requirements to secure organizational standing: “(1) that its members would have standing to sue as individuals; (2) that the interests it seeks to protect are germane to the organization’s purpose; and (3) that the suit does not require the participation of individual

members. *Equity In Athletics, Inc. v. Dep't of Educ.*, 639 F.3d 91, 99 (4th Cir. 2011) (citing *Hunt v. Washington State Apple Advertising Comm'n*, 432 U.S. 333, 343 (1977)).

B. Preliminary Injunction

A preliminary injunction is “an extraordinary remedy . . . which is to be applied ‘only in [the] limited circumstances’ which clearly demand it.” *Direx Israel, Ltd. v. Breakthrough Med. Corp.*, 952 F.2d 802, 811 (4th Cir. 1991) (quoting *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 800 (3d Cir. 1989)). To obtain a preliminary injunction, Plaintiffs must establish that: (1) they are likely to succeed on the merits of the case; (2) they are likely to suffer irreparable harm in the absence of injunctive relief; (3) the balance of equities tips in the Plaintiffs’ favor; and (4) an injunction is in the public interest. *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). The final two factors “merge when the Government is the opposing party.” *Miranda v. Garland*, 34 F.4th 338, 365 (4th Cir. 2022) (quoting *Nken v. Holder*, 556 U.S. 418, 435 (2009)).

III. ANALYSIS

The Court will first address the threshold issue of standing, before turning to the merits of Plaintiffs’ motion for injunctive relief.

A. Standing

As a threshold matter, Plaintiffs’ standing to pursue their claims appears, at best, questionable in the context of seeking injunctive relief; the Complaint does not appear to allege concrete harm resulting from Defendants’ actions that would satisfy the injury in fact requirement. To establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). To be “concrete,” the injury “must actually exist”—meaning it is “real” and “not abstract.” *Spokeo, Inc.*, 578 U.S. at

340. “For an injury to be ‘particularized,’ it ‘must affect the plaintiff in a personal and individual way.’” *Id.* at 339. “And while it is true that threatened rather than actual injury can satisfy Article III standing requirements, not all threatened injuries constitute an injury-in-fact. Rather, as the Supreme Court has emphasized repeatedly, an injury-in-fact must be concrete in both a qualitative and temporal sense.” *Beck v. McDonald*, 848 F.3d 262, 271 (4th Cir. 2017) (internal quotation marks and citations omitted).

Plaintiff Doe 1 alleges that she is a career civil servant. Dkt. 7 at 24. As such, OPM retains her personal information on EHRI, including her Social Security number, home address, and disciplinary record. *Id.* Plaintiffs also allege that Doe 1 and many of EPIC’s members have filed federal tax returns electronically within the last six years. *Id.* As a result, the BFS systems contain extensive financial information about them, including statutorily protected return information. *Id.* Plaintiffs further allege that they “reasonably expected that the information they provided the government was subject to comprehensive protections and against unlawful disclosure.” *Id.* Finally, Plaintiffs assert that the Government Defendants’ alleged disclosure of Plaintiffs’ personal information to the DOGE Defendants violates the Privacy Act and the Internal Revenue Code, injuring “Plaintiffs in a way that ‘creates statutory harm and confers standing.’” *Id.* (quoting *Gaston v. LexisNexis Risk Sols., Inc.*, 483 F. Supp. 3d 318, 343 (W.D.N.C. 2020)).

In contrast, Defendants contend that Plaintiffs have failed to demonstrate injury-in-fact because “there has been no third-party or unauthorized disclosure at Treasury or OPM, as only authorized agency employees have accessed the data systems at issue.” Dkt. 19 at 11. But regardless of whether Defendants’ actions constitute unlawful disclosure under the Privacy Act or the Internal Revenue Code, Defendants argue that, under *TransUnion LLC v. Ramirez*, 594 U.S. 413, 427 (2021), Plaintiffs have not demonstrated that any such violation concretely harmed them.

Defendants correctly observe that the Supreme Court has made clear that “[o]nly those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court.” *TransUnion*, 594 U.S. at 427 (emphasis original). Thus, “[t]he intangible harm of enduring a statutory violation, standing alone, typically won't suffice under Article III—unless there's separate harm (or a materially increased risk of another harm) associated with the violation.” *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 243 (4th Cir. 2023).

The Complaint does not allege harm separate from the alleged statutory violation of disclosure. Instead, Plaintiffs assert a heightened risk of harm, which falls short due to the speculative nature of any future injury. Specifically, Plaintiffs allege that the “ongoing breach of Treasury and OPM systems puts Plaintiffs at severe continuous risk of further data disclosure” and that there is “increased vulnerability to exfiltration by actors unaffiliated with the federal government or DOGE” because “OPM and Treasury data are rich targets for cyberattacks both by criminals and by foreign adversaries.” Dkt 1 ¶¶ 97, 100-01. However, Plaintiffs’ fear of harm from future exfiltration of their data by bad actors “relies on a highly attenuated chain of possibilities, [and] does not satisfy the requirement that threatened injury must be certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 410 (2013); *see also Beck*, 848 F.3d at 275 (explaining that “for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same ‘attenuated chain of possibilities’ rejected by the [Supreme] Court in *Clapper*”).

This Court appreciates that intangible harms can be concrete if they have a “close relationship to harms traditionally recognized as providing a basis for a lawsuit in American courts.” *TransUnion*, 594 U.S. at 425; *see also Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 295

(4th Cir. 2024). “That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury.” *TransUnion*, 594 U.S. at 424.

Endeavoring to align their claims with recognized legal harms, Plaintiffs contend in their Reply Brief that they have suffered an injury that is analogous to the common law tort of “intrusion upon seclusion,” Dkt. 20 at 9, which the Supreme Court has recognized as providing a basis for standing in federal lawsuits, *TransUnion*, 594 U.S. at 424. By definition, intrusion upon seclusion is the intentional intrusion, “physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.” Restatement (Second) of Torts, § 652B (Am. L. Inst. 1977); *see also Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 653 (4th Cir. 2019). The Court pauses to note that there is a dearth of case law on this subject—neither the parties nor the Court have found cases in this Circuit applying the common law tort of intrusion upon seclusion in similar circumstances to establish Article III standing following *TransUnion*. *Cf. O’Leary v. TrustedID, Inc.*, 60 F.4th 240, 245-46 (4th Cir. 2023) (holding that the plaintiff failed to allege injury with close relationship to intrusion upon seclusion because the plaintiff *chose* to hand over his partial social security number, and it is “the unwanted intrusion . . . that marks intrusion upon seclusion”). Comment (b) to Section 652B of the Second Restatement is informative, however, explaining that the invasion may be “by some other form of investigation or examination into [one’s] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.” Restatement (Second) of Torts, § 652B (Am. L. Inst. 1977). Further, “the intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the . . . information outlined.” *Id.*

Plaintiffs argue that the DOGE Defendants “have intentionally intruded upon Plaintiffs’ private information through large-scale unlawful data access,” and “the corresponding infringement on Plaintiffs’ privacy has a ‘close relationship,’ . . . to the harm traditionally recognized as the basis for an intrusion upon seclusion suit.” Dkt. 20 at 8 (quoting *Fernandez*, 116 F.4th at 295). Although Defendants did not have an opportunity to address this theory of standing during briefing, Defendants argued during the February 21, 2025 hearing that, assuming the common law tort applies (which Defendants do not concede that it does), a reasonable person would not be highly offended by an employee of Treasury or OPM accessing data on the agencies’ information systems in order to carry out the directives of an Executive Order.

For our purposes, the Court acknowledges that a practicable theory of standing under *TransUnion* based on the common law tort of intrusion upon seclusion may be sustainable. Nevertheless, given the lack of guidance on the application of this particular tort theory to establish standing in similar circumstances and the fact that Defendants have not had a meaningful opportunity to address this theory of standing, the Court declines to rule on the issue at this stage.

Thus, for the limited purposes of analyzing Plaintiffs’ Motion for injunctive relief, the Court will assume, without deciding, that Plaintiffs have standing in this case.

B. Preliminary Injunction

Turning to the Plaintiffs’ Motion for injunctive relief, the Court begins its analysis with irreparable harm, as “[t]he basis of injunctive relief in the federal courts has always been irreparable harm and inadequacy of legal remedies.” *Direx Israel, Ltd. v. Breakthrough Med. Corp.*, 952 F.2d 802, 812 (4th Cir. 1991) (quoting *Samson v. Murray*, 415 U.S. 61, 88 (1974)). Plaintiffs must make a “clear showing” of irreparable harm, demonstrating that the harm is “neither remote nor speculative, but actual and imminent.” *Direx*, 952 F.2d at 812 (internal quotation

omitted). Thus, a mere possibility of harm will not suffice. *See Winter*, 555 U.S. at 22 (“Issuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with our characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief.”).⁴

In their Motion, Plaintiffs argue that “[t]he longer Defendants are permitted unauthorized access to these sensitive systems, the more likely it is that they will access or further disclose Plaintiffs’ individual data, and the longer Plaintiffs’ data remains at a heightened risk of exposure or exfiltration by hostile actors.” Dkt. 7 at 24. Plaintiffs further allege that Defendants “can easily and immediately misuse [personal identifying information] in violation of law by arbitrarily stopping payments through access to the BFS system, as they have publicly claimed to do,” or by “bring[ing] adverse employment actions on the basis of information in the OPM system.” *Id.* at 26. Finally, Plaintiffs allege that there is a substantial risk of Plaintiffs suffering future identity theft because OPM’s network is regularly subject to hacking attempts, and that these attempts are more likely to be successful as a result of Defendants’ actions. *Id.* at 27. The Court is unpersuaded.

Plaintiffs’ fears of future harm are much too speculative and would require the Court to make several leaps in reasoning in order to warrant injunctive relief. For instance, Plaintiffs have not provided concrete evidence that Defendants are actively misusing or even attempting to misuse

⁴ This Court recognizes that under 26 U.S.C. § 6103, tax “[r]eturns and return information shall be confidential, and . . . no officer or employee of the United States . . . shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee” “Congress has carefully delineated the circumstances in which returns or return information can be disclosed to government officials or to the public.” *In re U.S.*, 817 F.3d 953 (6th Cir. 2016). Accordingly, disclosure of such information stemming from BFS and/or EHRI by any unauthorized personnel could be a concrete harm by which Plaintiffs could seek relief, – and this Court warns that any such violation of Section 6103 could result in potential criminal liability for said personnel. 26 U.S.C. § 6103.

their sensitive data.⁵ The hypothetical scenarios that Defendants will withhold payments or bring adverse employment actions based on Plaintiffs' sensitive data are unsupported by the record before this Court.⁶ And to accept Plaintiffs' argument based on the exfiltration of their information by hostile actors, the Court would have to conclude that Defendants' conduct is causing an increased likelihood of hacking, that any resulting breach would target the specific systems containing Plaintiffs' information, that Plaintiffs' information would be specifically targeted, and that such a breach would lead to identity theft or other tangible harm, economic or otherwise. This speculative chain of events is insufficient to establish irreparable harm, as Plaintiffs' claims are based on a series of possibilities, any one of which may never materialize. *See Beck*, 848 F.3d at 275 (referring to the plaintiffs' fear of identity theft as an "attenuated chain of possibilities" where the court had to "assume that the thief targeted the stolen items for the personal information they contained" and then assume that the thieves would "select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities"). "As the Supreme Court noted in *Winter*, the possibility of irreparable harm does not

⁵ Plaintiffs initially alleged that retired Lt. Gen. Mike Flynn tweeted sensitive information that could have only been obtained from access to BFS systems. Dkt. 1 ¶¶ 65-67. Plaintiffs have since submitted a notice stating that they have verified that the information contained in the Flynn tweet can be obtained from public sources. Dkt. 18 at 2. The Court appreciates this critical correction of the record.

⁶ The status updates from X/Twitter, upon which Plaintiffs rely to show that the DOGE Defendants have threatened to withhold payments that Plaintiffs are entitled to using the BFS system, only demonstrate that the DOGE Defendants were seeking to stop "improper" or "illegal" payments, not that the DOGE Defendants had access to sensitive information stored in the BFS systems or were targeting proper payments to Plaintiffs. *See, e.g.*, Dkt. 7 at 12 (stating that Musk tweeted that "The @DOGE team is rapidly shutting down these illegal payments" and that the DOGE X/Twitter account stated that it was "stopping improper payments").

constitute a ‘clear showing’ that the plaintiff is entitled to relief.” *Di Biase v. SPX Corp.*, 872 F.3d 224, 235 (4th Cir. 2017).⁷

Given the extraordinary nature of the remedy and the speculative, attenuated nature of the potential harm that Plaintiffs face, the Court cannot issue injunctive relief based on the current record before it.⁸

IV. CONCLUSION


In sum, while the Court does not definitively resolve the standing issue, even assuming Plaintiffs have standing, the Motion for injunctive relief is denied based on the failure to establish irreparable harm. Accordingly, for the foregoing reasons, it is hereby

ORDERED that Plaintiffs’ Motion for Temporary Restraining Order (Dkt. 5) is CONVERTED to a Motion for Preliminary Injunction; and it is

FURTHER ORDERED that Plaintiffs’ Motion for Preliminary Injunction (Dkt. 5) is DENIED.

It is SO ORDERED.

Alexandria, Virginia
February 21, 2025



/s/ Rossie D. Alston, Jr.
United States District Judge

⁷ Given that Plaintiffs have not met their burden in demonstrating irreparable harm, the Court need not address the remaining preliminary injunction factors.

⁸ Although the Court is denying injunctive relief based on the current record, Plaintiffs are permitted to take necessary action to protect their rights if, in the future, they experience harm that is more concrete and immediate, including if Plaintiffs are able to provide evidence that unauthorized personnel accessed the BFS and/or EHRI systems.