UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BECKY WELBORN, *et al.*,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	**Civil Action No. 15-1352 (RMC)**
	)	
INTERNAL REVENUE SERVICE, *et al.*,	)	
	)	
Defendants.	)	
	)	

OPINION

Becky Welborn, Wendy Windrich, and Beth DuPree, on behalf of a proposed class, allege that the Internal Revenue Service, IRS Commissioner John A. Koskinen, and IRS employees, identified as Does 1-100, violated their rights under the Privacy Act, 5 U.S.C. § 552a; the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.*; and the Internal Revenue Code, 26 U.S.C. § 6103, by disclosing or failing to prevent the disclosure of their personal identification information to third parties. The Defendants have filed a motion to dismiss, which is meritorious. The Complaint will be dismissed.

I.

A. Background

The IRS administers and enforces the U.S. tax code. The Commissioner's role is to "ensure[] that the agency maintains an appropriate balance between taxpayer service and tax enforcement and administers the tax code with fairness and integrity." Am. Compl. [Dkt. 22] ¶ 29. In that role, the Commissioner is "responsible for establishing and interpreting tax administration policy and for developing strategic issues, goals and objectives for managing and operating the IRS." *Id.*

The IRS "maintains a significant amount of personal and financial information" on each taxpayer and is, therefore, obligated to protect the confidentiality of that information. *Id*. ¶ 36. The Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 *et seq.*, "was enacted to strengthen the security of information and systems within federal government agencies," such as the IRS. Am. Compl. ¶ 36. FISMA requires federal agencies to evaluate periodically the "agency's information security programs and practices." *Id*. ¶ 37. FISMA specifically requires:

> (1) annual agency program reviews; (2) annual Inspector General evaluations; (3) agency reporting to the Office of Management and Budget ("OMB") the results of Inspector General evaluations for unclassified software systems; and (4) an annual OMB report to Congress summarizing the material received from agencies.

Id. To assist Inspectors General in evaluating agency systems, the Department of Homeland Security (DHS) specified eleven (11) information-security program areas and listed the specific attribute(s) within each area that should be evaluated. The eleven areas that were identified for evaluation under FISMA comprised:

> (1) continuous monitoring management; (2) configuration management; (3) identity and access management; (4) incident and response reporting; (5) risk management; (6) security training; (7) plan of action and milestones; (8) remote access management; (9) contingency planning; (10) contractor systems; and (11) security capital planning.

Id. The Treasury Inspector General for Tax Administration (TIGTA) is responsible for evaluations of the information security programs at the Department of Treasury, including the IRS. In its Fiscal Year 2014 FISMA report, TIGTA "found four security programs that were not fully effective due to one or more DHS guideline program attributes that were not met," *id*. ¶ 42, and that two security program areas "did not meet the level of performance specified by the DHS guidelines due to the majority of the specified attributes not being met," *id*. ¶ 43.

The President signed the Federal Information Security Modernization Act of 2014 ("Modernization Act") into law on December 18, 2014. Pub. L. No. 113-283, 128 Stat. 3073 (2014). This statute amended FISMA, retaining the authority of the Director of the Office of Management and Budget for oversight and authorizing the Secretary of DHS to administer its implementation by way of improved security policies and practices across the Executive Branch.

B. Breach of the IRS "Get Transcript" On-Line Program

The IRS launched the Get Transcript online application in January 2014 to allow "taxpayers to view and print a copy of their prior-year tax information." Am. Compl. ¶ 31. The purpose of Get Transcript was "to provide taxpayers with self-service and electronic service options in the form of web-based tools." *Id*. During the 2015 filing season, the Get Transcript software tool was used by taxpayers "to obtain approximately 23 million copies of their recently filed tax information." *Id*. ¶ 61. The IRS noticed unusual activity in the Get Transcript system in mid-May 2015, which led to the discovery of "questionable attempts to access the Get Transcript application." *Id*. Get Transcript was shut down on May 21, 2015.

Upon further investigation, the IRS discovered that 330,000 tax-related documents were stolen during a cyber attack that extended from mid-February to mid-May 2015. *Id*. Plaintiffs allege that the Commissioner reported to the U.S. Senate Finance Committee on June 2, 2015 that "hackers made 200,000 attempts on the 'Get Transcript' page, approximately half of which were successful." *Id.* ¶ 5 (emphasis removed). According to reports from the IRS, one or more individuals succeeded in bypassing the program's authentication process to access taxpayer records. *Id*. ¶ 62. The information stolen included a wide range of taxpayer information, including personal identification information (identified by the parties as "PII").

Plaintiffs further allege that TIGTA had recommended greater security on Get Transcript but the IRS chose "to roll out a more simple authentication method to encourage use," despite knowing that it "was vulnerable and insecure." *Id.* ¶¶ 12-13.

C. Plaintiffs' Private Data

In June 2015, Ms. Windrich learned of fraud arising from the mis-use of her tax records when she received a letter from the IRS informing her that an electronic tax return had been processed and a refund deposited, although Ms. Windrich had submitted her tax return via the U.S. Postal Service. As a result, Ms. Windrich and her husband "spent more than 30 hours dealing with the ramifications." *Id*. ¶ 76. Ms. Windrich "reasonably believes that her PII was compromised and obtained by the cybercriminals through the IRS systems." *Id.* The IRS now prohibits her and her husband from submitting electronic tax returns and she alleges that she "is at a heightened risk of further identity theft requiring her to pay indefinitely for on-going credit monitoring." *Id*.

Over the summer of 2015, Ms. Welborn was alerted to possible fraud through a duplicate joint tax return that an unknown person or persons submitted to the IRS in her name. As a result, Ms. Welborn and her husband also "spent dozens of hours dealing with the ramifications." *Id*. ¶ 83. Ms. Welborn "had to change all of their bank account numbers, file a police report, place fraud alerts with all three credit agencies, file a report with the Federal Trade Commission, submit a fraud affidavit to the IRS, and request written copies of her family's credit reports from the three credit agencies." *Id*. As is Ms. Windrich, Ms. Welborn is now prohibited by the IRS from submitting her tax returns online. She alleges that she "is at a heightened risk of further identity theft requiring her to pay indefinitely for on-going credit monitoring." *Id*. ¶ 84.

Ms. DuPree "was notified by a letter dated August 31, 2015 from the IRS that criminal actors potentially used her personal information to view her tax information through the IRS's Get Transcript application on IRS.gov." *Id*. ¶ 85. Ms. DuPree and her husband "spent numerous hours dealing with the ramifications," *id*. ¶ 89; specifically, Ms. DuPree "has been the victim of at least two occasions of fraudulent activity in her financial accounts . . . after the IRS data breach," *id*. Ms. DuPree "had to hire an attorney to investigate the fraudulent activity," is no longer eligible for electronic tax return filing, and alleges that she "is at a heightened risk of further identity theft requiring her to pay indefinitely for on-going credit monitoring." *Id*. ¶¶ 90-91. Overall,

> Plaintiffs request damages to compensate them for their current and future losses and injunctive relief to fix the IRS's security protocol, implement TIGTA's audit recommendations, implement President Obama's executive order focused on improving the security of consumer financial transactions, to [sic] provide adequate credit monitoring services for a sufficient time period, and to [sic] provide after-the-fact identity repair services and identity theft insurance to protect Class members from fraud and/or identity theft.

Id. ¶ 15.

D. Procedural History

Plaintiffs filed an Amended Class Action Complaint on January 6, 2016 seeking damages and injunctive relief. *See* Am. Compl. [Dkt. 22]. Plaintiffs allege that (1) Defendants violated the Privacy Act by intentionally and willfully failing to comply with FISMA and the Modernization Act, thereby allowing the disclosure of Plaintiffs' personal identifying information; (2) Defendants' failures to comply with FISMA and the Modernization Act were arbitrary and capricious, or otherwise violated the Administrative Procedure Act (APA); and (3) Defendants violated the Internal Revenue Code (Code) by disclosing, or allowing the disclosure of, Plaintiffs' personal identifying information to criminals. Plaintiffs intend their suit to be a

class action and define that class as "[a]ll Tax filers of the United States and their spouses and/or dependents whose PII was compromised as a result of the 'Get Transcript' application data breach." *Id*. ¶ 92.

Defendants moved to dismiss the Amended Complaint for lack of subject matter jurisdiction, Fed. R. Civ. P. 12(b)(1), and, in the alternative, for failure to state a claim upon which relief may be granted, Fed. R. Civ. P. 12(b)(6). *See* Mot. [Dkt. 24]. Plaintiffs have opposed that motion, *see* Opp'n [Dkt. 29], and Defendants filed a timely reply. *See* Reply [Dkt. 30]. The motion is ripe for review.

E. Jurisdiction and Venue

The Court has jurisdiction over the Privacy Act claims pursuant to 5 U.S.C. § 552a(g)(1), the APA claims pursuant to 28 U.S.C. § 1331, and the Internal Revenue Code claims pursuant to 26 U.S.C. § 6103. Venue is proper pursuant to 28 U.S.C. § 1391(e)(1).

II.

A. Motion to Dismiss

1. Rule 12(b)(1)

Federal Rule of Civil Procedure 12(b)(1) allows a defendant to move to dismiss a complaint, or any portion thereof, for lack of subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). No action of the parties can confer subject matter jurisdiction on a federal court because subject matter jurisdiction is both a statutory requirement and an Article III requirement. *Akinseye v. District of Columbia*, 339 F.3d 970, 971 (D.C. Cir. 2003). The party claiming subject matter jurisdiction bears the burden of demonstrating that such jurisdiction exists. *Khadr v. United States*, 529 F.3d 1112, 1115 (D.C. Cir. 2008); *see Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994) (noting that federal courts are courts of limited jurisdiction and

"[i]t is to be presumed that a cause lies outside this limited jurisdiction, and the burden of establishing the contrary rests upon the party asserting jurisdiction").

When reviewing a motion to dismiss for lack of jurisdiction under Rule 12(b)(1), a court must review the complaint liberally, granting the plaintiff the benefit of all inferences that can be derived from the facts alleged. *Barr v. Clinton*, 370 F.3d 1196, 1199 (D.C. Cir. 2004). Nevertheless, "the Court need not accept factual inferences drawn by plaintiffs if those inferences are not supported by facts alleged in the complaint, nor must the Court accept plaintiffs' legal conclusions." *Speelman v. United States*, 461 F. Supp. 2d 71, 73 (D.D.C. 2006). A court may consider materials outside the pleadings to determine its jurisdiction. *Settles v. U.S. Parole Comm'n*, 429 F.3d 1098, 1107 (D.C. Cir. 2005); *Coal. for Underground Expansion v. Mineta*, 333 F.3d 193, 198 (D.C. Cir. 2003). A court has "broad discretion to consider relevant and competent evidence" to resolve factual issues raised by a Rule 12(b)(1) motion. *Finca Santa Elena, Inc. v. U.S. Army Corps of Eng'rs*, 873 F. Supp. 2d 363, 368 (D.D.C. 2012) (citing 5B Charles Wright & Arthur Miller, Fed. Prac. & Pro., Civil § 1350 (3d ed. 2004)); *see also Macharia v. United States*, 238 F. Supp. 2d 13, 20 (D.D.C. 2002), *aff'd*, 334 F.3d 61 (2003) (in reviewing a factual challenge to the truthfulness of the allegations in a complaint, a court may examine testimony and affidavits). In such circumstances, consideration of documents outside the pleadings does not convert the motion to dismiss into one for summary judgment. *Al-Owhali v. Ashcroft*, 279 F. Supp. 2d 13, 21 (D.D.C. 2003).

2. Rule 12(b)(6)

A motion to dismiss for failure to state a claim under Fed. R. Civ. P. 12(b)(6) challenges the adequacy of a complaint on its face. Fed. R. Civ. P. 12(b)(6) ("Every defense to a claim for relief in any pleading must be asserted in the responsive pleading if one is required.

But a party may assert the following defenses by motion: . . . (6) failure to state a claim upon which relief can be granted[.]"). To survive a motion to dismiss, a complaint must contain sufficient factual information, accepted as true, to "'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A court must assume the truth of all well-pleaded factual allegations and construe reasonable inferences from those allegations in favor of the plaintiff. *Sissel v. Dep't of Health & Human Servs.*, 760 F.3d 1, 4 (D.C. Cir. 2014). A court need not accept inferences drawn by a plaintiff if such inferences are not supported by the facts set out in the complaint. *Kowal v. MCI Commc'ns Corp.*, 16 F.3d 1271, 1276 (D.C. Cir. 1994). Further, a court does not need to accept as true legal conclusions set forth in a complaint. *Iqbal*, 556 U.S. at 678. In deciding a motion under Rule 12(b)(6), a court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits or incorporated by reference, and matters about which the court may take judicial notice. *Abhe & Svoboda, Inc. v. Chao*, 508 F.3d 1052, 1059 (D.C. Cir. 2007).

B. Privacy Act

The Privacy Act "safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records by allowing an individual to participate in ensuring that his records are accurate and properly used." *Henke v. Dep't of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996); *see also FAA v. Cooper*, 132 S. Ct. 1441, 1446 (2012) (noting the "comprehensive and detailed set of requirements" laid out in the Privacy Act to protect individuals' personal information). The Privacy Act specifically prohibits disclosure of "any record which is contained in a system of records by any means of communication to any person, or to another agency" without the consent of the individual to

whom the record pertains or disclosure is otherwise authorized under the Privacy Act. 5 U.S.C. § 552a(b). A record is defined as:

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

5 U.S.C. § 552a(a)(4). A system of records includes "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5). In addition to prohibiting disclosure, the Privacy Act requires agencies to secure records by:

> establish[ing] appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

5 U.S.C. § 552a(e)(10).

District courts have jurisdiction over civil actions brought by individuals who have been adversely affected by a violation of the Privacy Act. See 5 U.S.C. § 552a(g)(1). Relief is tied to the nature of the violation alleged. Monetary damages are permitted in suits brought under § 552a(g)(1)(C) or (D) when "the agency acted in a manner which was intentional or willful." 5 U.S.C. § 552a(g)(4). Section 552(g)(1)(D) permits monetary damages when an agency "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual." 5 U.S.C. § 552a(g)(1)(D).

C. Administrative Procedure Act

The APA requires a reviewing court to set aside an agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A); *Tourus Records, Inc. v. Drug Enforcement Admin.*, 259 F.3d 731, 736 (D.C. Cir. 2001). A claim under the APA can challenge agency action or "fail[ure] to act." 5 U.S.C. § 702. While the APA allows a court to compel agency action, it excludes agency action that "is committed to agency discretion by law." 5 U.S.C. § 701(a)(2).

In reviewing agency action, a court "must consider whether the [agency's] decision was based on a consideration of the relevant factors and whether there has been a clear error of judgment." *Marsh v. Oregon Natural Res. Council*, 490 U.S. 360, 378 (1989) (internal quotation marks omitted). At a minimum, the agency must have considered relevant data and articulated an explanation establishing a "rational connection between the facts found and the choice made." *Bowen v. Am. Hosp. Ass'n*, 476 U.S. 610, 626 (1986); *see also Pub. Citizen, Inc. v. Fed. Aviation Admin.*, 988 F.2d 186, 197 (D.C. Cir. 1993) ("The requirement that agency action not be arbitrary or capricious includes a requirement that the agency adequately explain its result."). An agency action usually is arbitrary or capricious if

> the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Motor Vehicle Mfrs. Ass'n of U.S.v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983); *see also County of Los Angeles v. Shalala*, 192 F.3d 1005, 1021 (D.C. Cir. 1999) ("Where the agency has failed to provide a reasoned explanation, or where the record belies the agency's conclusion, [the court] must undo its action.").

As the Supreme Court has directed, "the scope of review under the 'arbitrary and capricious' standard is narrow and a court is not to substitute its judgment for that of the agency." *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43. Rather, the agency action under review is "entitled to a presumption of regularity." *Citizens to Pres. Overton Park, Inc. v. Volpe*, 401 U.S. 402, 415 (1971), *abrogated on other grounds by Califano v. Sanders*, 430 U.S. 99 (1977). If the district court can "reasonably discern" the agency's path, it should uphold the agency's decision. *Pub. Citizen*, 988 F.2d at 197.

D. Internal Revenue Code

The Code provides for the protection of tax returns and return information and authorizes civil suit and remedies for unauthorized disclosure of such information. Section 6103 provides that "[r]eturns and return information shall be confidential" and not disclosed unless authorized under the Code. 26 U.S.C. § 6103(a). The Code allows a civil action for improper disclosure when "any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103." 26 U.S.C. § 7431(a)(1). Section 6103 states that disclosure "means the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8). "Returns and return information" is broadly defined to include everything from a completed tax return submitted by a taxpayer to "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, . . . or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return." 26 U.S.C. § 6103(b)(1), (b)(2)(A). If a plaintiff succeeds on a claim under § 7431, they may receive:

> (1) the greater of—
>
> (A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or
>
> (B) the sum of—(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus (ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus
>
> (2) the costs of the action, plus
>
> (3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

26 U.S.C. § 7431(c).

III.

A. Do Plaintiffs Have Standing to Sue?

Standing is part and parcel of Article III's limitation on the judicial power of the federal courts and extends only to cases or controversies. U.S. Const. art. III, § 2 ("The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority [and] to Controversies . . . ."); *Ariz. State Legislature v. Ariz. Indep. Redistricting Comm'n*, 135 S. Ct. 2652, 2663 (2015). The strictures of Article III standing are by now "familiar." *United States v. Windsor*, 133 S. Ct. 2675, 2685 (2013). Standing requires (1) the plaintiff to have suffered an injury in fact that is both (a) concrete and particularized and (b) actual or imminent, as opposed to conjectural or hypothetical; (2) the injury must be traceable to the defendants' actions; and (3) the injury must be redressable by a favorable decision of the court. *See id*. at 2685-86 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-62 (1992)). In the context of a putative class

action, all named plaintiffs "must allege and show that they *personally* have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975) (emphasis added).

A federal court must assure itself of both constitutional and statutory subject matter jurisdiction. The former obtains if the case is one "arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority." U.S. Const. art. III, § 2. The relevant statute, 28 U.S.C. § 1331, likewise confers jurisdiction upon lower courts to hear "all civil actions arising under the Constitution, laws, or treaties of the United States." Federal courts have constitutional and statutory "arising under" jurisdiction whenever a plaintiff's claim "will be sustained if the Constitution is given one construction and will be defeated if it is given another." *Powell v. McCormack*, 395 U.S. 486, 514-16 (1969) (citing *Bell v. Hood*, 327 U.S. 678, 685 (1946) and *King Cnty. v. Seattle Sch. Dist. No. 1*, 263 U.S. 361, 363-64 (1923)).

1. Injury-in-Fact

A plaintiff must allege an injury-in-fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. *See Windsor*, 133 S. Ct. at 2685 (citing *Lujan*, 504 U.S. at 559-62). Allegations of speculative or possible future injury do not satisfy the requirements of Article III. "A threatened injury must be certainly impending to constitute injury in fact." *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (internal quotations omitted).

When an alleged injury has not yet occurred, courts must determine whether it is imminent. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013). An injury is imminent if the threatened injury is "certainly impending" or if there is substantial risk that the harm will occur. *Id*. "[P]laintiffs bear the burden of pleading . . . concrete facts showing that the

defendant's actual action has caused the substantial risk of harm. Plaintiffs cannot rely on speculation about the unfettered choices made by independent actors not before the court." *Id*. at 1150 n. 5 (internal quotation and citation omitted). Plaintiffs also "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id*. at 1151.

Defendants argue that Plaintiffs Welborn and Windrich have failed to allege an injury-in-fact sufficient to satisfy the requirements for standing under Article III. In this regard, Defendants contend: (1) the filing of fraudulent tax returns by a criminal; (2) the risk of future economic harm; (3) the costs to monitor and evaluate their credit; and (4) the alleged diminished value of these Plaintiffs' personal identifying information are not legally cognizable injuries. Plaintiffs respond that Mses. Welborn and Windrich adequately plead injury-in-fact because they suffered actual identity theft in the form of false tax returns filed in their names and that, due to the substantial risk of future economic harm, they have already reasonably incurred costs to evaluate and mitigate that risk.

Plaintiffs cite *In re Science Applications International Corp. Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (*SAIC*), which the Court finds instructive here. *SAIC* concerned the theft of a backup tape that contained the names and social security numbers of 4.7 million members of the U.S. military and their families. In the many subsequent lawsuits against the government and SAIC, a government contractor from whom the tape was stolen, the plaintiffs plead the risk of future harm and the costs to monitor their credit and prevent future harm as cognizable injuries-in-fact. Judge James E. Boasberg of this Court evaluated each Plaintiff's standing in light of *Clapper v. Amnesty International USA*, 135 S. Ct. 1138 (2013), and held that neither the risk of future identity theft nor costs to monitor and

prevent future harm conferred Article III standing. In comparison, as to those *SAIC* plaintiffs who had already suffered instances of identity theft, the court found a clear injury that supported standing to sue. 45 F. Supp. 3d at 25. Because Mses. Welborn and Windrich both allege that they have suffered actual identity theft when someone filed false tax returns (and claimed fraudulent refunds) in their names, each of these Plaintiffs has plead sufficient injury-in-fact to establish standing. *See* Am. Compl. ¶¶ 71-73, 79. As the IRS does not dispute that Ms. DuPree has alleged an injury in fact—she "has been the victim of at least two occasions of fraudulent activity in her financial accounts, one of which resulted in the removal of funds from a personal financial account, which occurred after the IRS data breach," *id*. ¶ 89—all three Plaintiffs have alleged sufficient injury-in-fact.

Plaintiffs' other alleged injuries are too ephemeral to suffice under *Clapper*. Plaintiffs rest largely on the theory that they suffer an increased threat of future identity theft and fraud as a result of the IRS security breach. *See id*. ¶¶ 76, 83-84, 90-91; Opp'n at 15. *Clapper* has already instructed that a party cannot claim injury-in-fact based on hypothetical future harm that is not "certainly impending." 133 S. Ct. at 1143; *see also Whitmore*, 495 U.S. at 158. Plaintiffs have not alleged facts from which a plausible inference could be drawn that they face imminent harm that is "certainly impending." The likelihood that any Plaintiff will suffer additional harm remains entirely speculative and depends on the decisions and actions of one or more independent, and unidentified, actor(s). *See Clapper*, 133 S. Ct. at 1150. Thus, Plaintiffs' allegations that they face an increased risk of future harm does not satisfy Article III.

In addition, general anxiety does not establish standing. *See* Am. Compl. ¶¶ 74 (alleging that "Plaintiff Windrich is reasonably concerned about her and her husband's future"); 81 (alleging that "Plaintiff Welborn is reasonably concerned about her and her husband's future

. . . as the family's PII was in their stolen tax data"); and 88 (alleging that "Plaintiff DuPree is reasonably concerned about her and her spouse's . . . future"). An "objectively reasonable likelihood" of future harm does not establish standing in the present time, despite legitimate anxiety that ill might befall an individual. *Clapper*, 133 S. Ct. at 1147-48. Even if their fears are rational, this uncertain and inchoate risk does not confer standing. *See SAIC*, 45 F. Supp. 3d at 26; *see also Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088 (E.D. Cal. 2015) (rejecting claim that theft of information established that plaintiff "suffers from a substantial risk of imminent future harm"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954-55 (D. Nev. 2015) (finding no standing where the last four digits of credit card numbers of 24 million customers were stolen, without allegations of unauthorized purchases or other signs of misuse).

Plaintiffs also allege injury based on the time and money spent monitoring and assessing the potential risk of future harm. *See* Am. Compl. ¶¶ 76, 83, 89. However, "the cost involved in *preventing* future harm" does not constitute an injury-in-fact. *SAIC*, 45 F. Supp. 3d at 26 (emphasis in original).

These legal maxims were clearly established in *Clapper*, if not before. The Supreme Court held that proactive measures based on "fears of . . . future harm that is not certainly impending" do not create an injury in fact, even where such fears are not unfounded. *Clapper*, 133 S. Ct. at 1151. In other words, Plaintiffs cannot create standing by "inflicting harm on themselves" to ward off a speculative future injury. *Id.*; *see also Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011) (finding that "Appellants' alleged time and money expenditures to monitor their financial information did not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more

'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims").

Finally, Plaintiffs claim as injury the "diminished value of their PII." Opp'n at 15. Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value. *See, e.g. Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 697 (7th Cir. 2015) (finding no standing from "such an abstract injury, particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 954; *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1029 (N.D. Cal. 2012) (finding such allegations "too abstract and speculative to support Article III standing").

If, contrary to the necessity of an injury-in-fact, one could assume that Plaintiffs' personal identifying information had economic value, Plaintiffs do not allege facts to support the inference of their allegation that their personal information became less valuable as a result of the IRS breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the breach. *See SAIC*, 45 F. Supp. 3d at 30; *Zappos.com*, 108 F. Supp. 3d at 954. These allegations do not establish an injury-in-fact.

2. Causation

Causation is the second element of standing and just as critical as an injury-in-fact. Causation requires "a causal connection between the injury and the conduct complained of." *Lujan*, 504 U.S. at 560. The harm alleged must be "fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court." *Bennett v. Spear*, 520 U.S. 154, 167 (1997). Because the fraud alleged here was committed by third parties and not Defendants, Plaintiffs must also allege facts to show that, absent the alleged unlawful actions by the IRS (in alleged violation of the Privacy Act, the APA

and/or the Code), "there is a substantial probability that they would not be injured.'" *Chamber of Commerce v. EPA*, 642 F.3d 192, 201 (D.C. Cir. 2011) (quoting *Warth*, 422 U.S. at 504). In other words, to demonstrate causation, Plaintiffs must put forward facts showing that their injuries can be traced to the specific data incident of which they complain and not to any previous theft or data loss incident. *See SAIC*, 45 F. Supp. 3d at 32. At a minimum, they must allege facts that indicate that the information stolen from the Defendants in the Get Transcript breach is the same type of information used to commit their injuries. *See id.* at 31-32.

Ms. Windrich alleges that "the IRS told her that the fraudulent tax return [filed in the Windriches' names] had very specific and personal information that had to be taken from her prior two years' income tax returns" and "the information supplied in the fraudulent tax return could only have come from the Get Transcript application." Am. Compl. ¶ 73. At the point of a motion to dismiss, a court credits all well-pled facts and gives a plaintiff the benefit of all reasonable inferences that might be drawn from such facts. *See Sissel*, 760 F.3d at 4. Ms. Windrich has alleged sufficient facts that, if proved, would tend to show that the information used in the fraudulent tax return was of the same type that was stolen from the Get Transcript application and, therefore, has plead the necessary causal connection.

Ms. Welborn alleges that an "IRS representative explained to [her] that someone had filed a duplicate joint [tax] return using her and her husband's social security numbers" and "that the fraudulent party had requested a transcript of Plaintiff Welborn's taxes through the Get Transcript application." Am. Compl. ¶ 79. Again, taking the well-pled factual assertions as true, the Court finds Ms. Welborn has also alleged a sufficient causal connection to support her standing to sue.

Finally, Ms. DuPree alleges: (1) that she "was notified by a letter dated August 31, 2015 from the IRS that criminal actors potentially used her personal information to view her tax information through the IRS's Get Transcript application"; (2) that she "has never been notified by any other entity that her PII had been compromised"; and (3) that she has been the victim of "at least two occasions of fraudulent activity in her financial accounts, one of which resulted in the removal of funds from a personal financial account, which occurred after the IRS data breach." *Id*. ¶¶ 85-86, 89. These allegations alone do not sufficiently connect the Get Transcript incident to the removal of funds from Ms. DuPree's account. It is not clear that the type of data obtained from the theft of Get Transcript information was necessarily used in the removal of funds. *See SAIC*, 45 F. Supp. 3d at 31. Ms. DuPree simply alleges that the alleged financial fraud happened *after* the Get Transcript breach. *See* Am. Compl. ¶ 89; *see also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012) (holding that "to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence").

Recognizing this problem, Ms. DuPree attempts to supplement the Amended Complaint by submitting a declaration with her opposition. *See* Declaration of Michele M. Vercoski (Vercoski Decl.) [Dkt. 29-1]. In appropriate cases, a district court may "dispose of a motion to dismiss for lack of subject matter jurisdiction under Fed. R. Civ. P. 12(b)(1) on the complaint standing alone. But where necessary, the court may consider the complaint supplemented by undisputed facts evidenced in the record, or the complaint supplemented by undisputed facts plus the court's resolution of disputed facts." *Herbert v. Nat'l Acad. of Scis.*, 974 F.2d 192, 197 (D.C. Cir. 1992); *but see Sloan v. Urban Title Sers., Inc.*, 689 F. Supp. 2d 94, 114 (D.D.C. 2010) (finding that plaintiff "cannot amend her complaint through her opposition

briefing"). However, when considering a motion to dismiss for lack of subject matter jurisdiction, a court cannot "'rely on conclusory or hearsay statements contained in the affidavits.'" *See Treiber v. Aspen Dental Mgmt., Inc.*, 94 F. Supp. 3d 352, 361 (N.D.N.Y. 2015) (quoting *J.S. ex rel. N.S. v. Attica Cent. Schs.*, 386 F.3d 107, 110 (2d Cir. 2004)).

The Vercoski Declaration is submitted by counsel for Ms. DuPree and advances hearsay and conclusory statements. Although counsel can swear to the existence of IRS letters due to her "personal knowledge" of the evidence in the case, Ms. Vercoski cannot attest to Ms. DuPree's conversations with others or her thoughts about the cause of fraudulent attempts on her retirement account. The Vercoski Declaration states that Ms. DuPree filed a police report and "explained that the IRS's data breach, which would have indicated her retirement account information, was responsible for the fraud." Vercoski Decl. ¶ 9. Besides the obvious hearsay, the phrase "would have indicated" is in the subjective tense and does not state a *fact*. The Court cannot assume a critical element to establish causation and standing. Ms. DuPree's allegations will be dismissed.

3. Redressability

The last element of standing is redressability, requiring that it "be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan*, 504 U.S. at 561 (internal quotations and citation omitted); *see also SAIC*, 45 F. Supp. 3d at 33. Mses. Welborn and Windrich claim injury based on a misuse of their personal identifying information to file a fraudulent tax return. Any harms might be redressed through a monetary award. Therefore, Mses. Welborn and Windrich have standing to sue for monetary damages.

4. Do Plaintiffs Have Standing to Obtain an Injunction Under the APA?

To allege a case or controversy justifying an injunction, a plaintiff must allege more than "past exposure to illegal conduct." *City of Los Angeles v. Lyons*, 461 U.S. 95, 102

(1983) (internal quotations and citation omitted). *City of Los Angeles v. Lyons* involved claims by Mr. Lyons that the L.A. police had unreasonably put him in a chokehold that injured his larynx. The D.C. Circuit has summarized the holding in *City of Los Angeles* to wit: "while Lyons could maintain a suit for damages, he could not maintain his suit for an injunction because he 'has made no showing that he is realistically threatened by a repetition of his experience.'" *Fair Emp't Council of Greater Washington, Inc. v. BMC Mktg. Corp.*, 28 F.3d 1268, 1272 (D.C. Cir. 1994) (discussing *City of Los Angeles*). "To pursue an injunction or a declaratory judgment, . . . plaintiffs must allege a likelihood of future *violations* of their rights by [the IRS], not simply future *effects* from past violations." *Id*. at 1273 (emphasis in original); *see also Dearth v. Holder*, 641 F.3d 499, 501 (D.C. Cir. 2011) (finding a plaintiff "must show he is suffering an ongoing injury or faces an immediate threat of [future] injury"); *Peterson v. Transp. Workers Union of Am., AFL-CIO*, 75 F. Supp. 3d 131, 136 n.2 (D.D.C. 2014) ("[A] plaintiff seeking a declaratory judgment must still present a 'substantial controversy . . . of sufficient immediacy and reality' in order to have standing.") (quoting *Fed. Exp. Corp. v. Air Line Pilots Ass'n*, 67 F.3d 961, 964 (D.C. Cir. 1995)).

This legal principle is well established. "[W]hen a plaintiff seeks injunctive or declaratory relief specifically for the purpose of challenging an alleged policy or practice of a government agency, the plaintiff must demonstrate that it is 'realistically threatened by a repetition of its experience.'" *Afifi v. Lynch*, 101 F. Supp. 3d 90, 108-09 (D.D.C. 2015) (quoting *Haase v. Sessions*, 835 F.2d 902, 910-11 (D.C. Cir. 1987)). Plaintiffs must plead a "real or immediate" threat of repetition, not merely "a nebulous assertion of the existence of a 'policy'" and a likelihood that they will "be subjected to the policy again." *Haase*, 835 F.2d at 911; *see also Lyons*, 461 U.S. at 102-06; *Golden v. Zwickler*, 394 U.S. 103, 109 (1969). Get Transcript

was withdrawn in May 2015 and Plaintiffs make no allegation that the IRS continues to allow access to their personal identifying information. The allegations that the IRS failed to comply with FISMA or the Modernization Act do not help. FISMA is a peculiarly hortatory statute directed to federal executives to protect federal information technology for the benefit of the federal government. There is no private right of action under FISMA or the Modernization Act and, indeed, each agency head is delegated full discretion in determining how to achieve its goals, which removes it from APA review. *See* 5 U.S.C. § 701(a) (permitting APA review "except to the extent that (1) statutes preclude judicial review; or (2) agency action is committed to agency discretion by law"); *see also Heckler v. Chaney*, 470 U.S. 821, 828 (1985). Plaintiffs have not established standing to sue for injunctive or other equitable relief under the APA and, therefore, Count 2 will be dismissed.[1]

B. Can Plaintiffs Maintain Their Claims of Unauthorized Disclosure Under the Privacy Act?

Defendants move to dismiss Plaintiffs' Privacy Act unauthorized disclosure claims because the Code preempts all Privacy Act claims for the unauthorized disclosure of tax returns and return information. Plaintiffs fail to respond, addressing only whether the Code preempts a Privacy Act claim that the IRS failed to "safeguard" their personal identity information. Opp'n at 26-27. The Court, like Defendants, will interpret Plaintiffs' Complaint as raising two separate types of Privacy Act claims and will dismiss the unauthorized disclosure claims because they are preempted by the Code. *See* 26 U.S.C. §§ 6103(a), 7431; *see also*

[1] In the alternative, the Court finds that the Privacy Act would preempt Plaintiffs' APA claims because the prior statute provides the only congressionally-intended legal remedy and neither injunctive relief nor any other equitable relief is available. "[I]f an adequate remedy at law exists, equitable relief is not available under the APA." *Cohen v. United States*, 650 F.3d 717, 731 (D.C. Cir. 2011).

Gardner v. United States, 213 F.3d 735, 742 (D.C. Cir. 2000) ("[Section] 6103 is the exclusive remedy for a taxpayer claiming unlawful disclosure of his or her tax returns and tax information."). Section 6103(a) precludes officers and employees of the United States (and others) from disclosing any return or return information. Disclosure "means the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8). Further, at § 7431, the Code specifically provides for civil damages in the event of unauthorized disclosure of returns and return information. 26 U.S.C. § 7431.

C. Failure to State a Claim

Defendants also seek dismissal of Plaintiffs' claims for failure to state a claim upon which relief may be granted. *See* Fed. R. Civ. P. 12(b)(6).

1. Privacy Act (Count 1)

Defendants argue that Plaintiffs' Privacy Act claims, both for improper disclosure and failure to safeguard, must be dismissed for failure to state a claim because Plaintiffs do not plead actual damages. Defendants explain that actual damages under the Privacy Act are equivalent to special damages under Federal Rule of Civil Procedure 9(a) and must be pled with specificity. *See FAA v. Cooper*, 132 S. Ct. at 1451-52 ("The basic idea is that Privacy Act victims, like victims of libel *per quod* or slander, are barred from any recovery unless they can first show actual—that is, pecuniary or material—harm."). In opposition, Plaintiffs argue they did plead actual damages in the form of (1) time spent addressing the data theft from the IRS, (2) credit monitoring costs, (3) costs associated with actual data theft, and (4) cancelled credit cards. Defendants reply that none qualifies as actual damages because none is a calculable monetary loss or "constitute[s] actual damages stemming from the Get Transcript incident." Reply at 14.

To plead any Privacy Act claim adequately, a plaintiff must plead "actual—that is, pecuniary or material—harm." *Cooper*, 132 S. Ct. at 1451. In this respect, there is no distinction between Plaintiffs' separate allegations of Privacy Act violations, whether unauthorized release of their private information or the alleged failure by the IRS to implement safeguards to protect their information. The Privacy Act does not allow a claim for damages based on reputational or emotional harm. *Id*. at 1454-56 ("[T]he Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress. Accordingly, the Act does not waive the Federal Government's sovereign immunity from liability for such harms."). As a result, Plaintiffs must specifically allege actual damages to survive a motion to dismiss for failure to state a claim.

The Court will not assume actual damages based on a conclusory statement that Plaintiffs and Class members "have suffered or are at increased risk of suffering from" a list of potential harms. Am. Compl. ¶ 69. Plaintiffs must specifically allege that they have suffered calcuable damages to survive Defendants' motion to dismiss. Plaintiffs allege the following injuries: (1) false tax returns were filed, (2) future prohibition from e-filing taxes, (3) lost time spent dealing with the ramifications of the fraud, and (4) heightened risk of further identity theft.[2] None of these allegations details actual pecuniary or material damage. Plaintiffs cite *Hill v. Department of Defense*, 70 F. Supp. 3d 17 (D.D.C. 2014), for the proposition that allegations

[2] In Opposition, Plaintiffs argue they suffered damages through "out-of-pocket expenses associated with the detection, investigation, and recovery after actual theft" and "economic loss due to cancelling credit cards." Opp'n at 36. These specific allegations, however, are not included in the Amended Complaint and, if they were, they do not allege actual damages. As explained in the discussion on standing, injury based on hypothetical future harm is not sufficient. *See Clapper*, 133 S. Ct. at 1143. The fact that Plaintiffs chose to spend money on credit monitoring services to prevent potential future harm does not allege actual damages attributable to the IRS. *See* 5 U.S.C. 552a(g)(4); *SAIC*, 45 F. Supp. 3d at 32.

of direct expenses, such as the time spent dealing with an injury, are sufficient to constitute actual damages. *Hill*, however, relied on allegations that the plaintiff made *actual* payments for medical treatment as a result of intense distress following the loss of her personal information. Plaintiffs make no equivalent allegations. Plaintiffs' Privacy Act claims for failure to safeguard their personal identifying information must be dismissed because they present no claim of actual damages and thereby fail to state a claim. This same analysis would apply to Plaintiffs' Privacy Act claims for unauthorized disclosure were they not precluded by the Code.[3]

2. Improper Disclosure under the Code

Defendants argue that Plaintiffs' allegations of improper disclosure under the Code fail to state a claim because Plaintiffs do not allege a disclosure by an IRS officer or employee to another individual. Plaintiffs answer that disclosure does not require person-to-person contact and it was, in this case, made by negligently giving access to return and return information through the unsecure Get Transcript application.

To allege improper disclosure under the Code, a plaintiff must allege (1) knowing or negligent, (2) disclosure, (3) of a return or return information in violation of § 6103. *See Fostvedt v. IRS*, 824 F. Supp. 978, 983 (D. Colo. 1993), *aff'd sub nom. Fostvedt v. United States*, 16 F.3d 416 (10th Cir. 1994) ("In order to recover under section 7431 for violations of section 6103, a taxpayer must show by a preponderance of the evidence that: (1) the disclosure was unauthorized; (2) the disclosure was made knowingly or by reason of negligence; and (3) the

[3] Defendants additionally argue that Plaintiffs failed to state a claim of improper disclosure under the Privacy Act because they have not argued that it was an "intentional or willful" disclosure by the IRS. To the contrary, Plaintiffs complain that the IRS intentionally and willfully failed to establish adequate security in the Get Transcript application and thereby exposed their personal identifying information to one or more hackers. *See* Am. Compl. ¶¶ 50-68. Nonetheless, the theft itself was caused by an unknown third party. *See In re Dep't of Veterans Affairs (VA) Data Theft Litig.*, No. 06-506, 2007 WL 7621261, at *5-6 (D.D.C. Nov. 16, 2007) ("The theft of the records does not give rise to a claim for unauthorized disclosure.").

disclosure violated section 6103." (internal quotations omitted)). Plaintiffs allege, without contest from Defendants, that their personal identifying information was in their tax returns and is the type of information as to which § 6103 precludes disclosure.

Defendants' argument relies on the Code definition of "disclosure," requiring disclosure by an IRS officer or employee. Defendants posit that disclosure by an IRS officer or employee was impossible on these facts because the disclosure was made through the Get Transcript application, an automated IRS system.

At § 7431(a)(2), the Code allows a cause of action against "any person who is *not* an officer or employee of the United States" if that person unlawfully discloses return information. 26 U.S.C. § 7431(a)(2) (emphasis added). A "person" is defined in the Code as "an individual, a trust, estate, partnership, association, company or corporation." 26 U.S.C. § 7701(a)(1). Based on this definition, *Marsoun v. United States*, 525 F. Supp. 2d 206, 213 (D.D.C. 2007) found that § 7431(a)(2) "does not authorize a right of action against a State, its agencies, or state employees sued in their official capacities (the latter, of course, being no different than a suit against the state)."

Defendants attempt to conflate § 7431(a)(2)'s cause of action against an individual not associated with the IRS and the cause of action against the United States permitted in § 7431(a)(1). Defendants offer no case law specifying that the disclosure considered under § 7431(a)(1) must be person-to-person. Disclosure is defined in § 6103(b)(8) as "making known to any person in any manner," not making known through personal transfer, which the IRS would ask this Court to require. Plaintiffs also specifically allege that an individual or individuals, Commissioner Koskinen and/or Does 1-100, are responsible for the disclosure through a failure to comply with FISMA and safeguard the Get Transcript application. To the

extent an individual is necessary, therefore, Plaintiffs have alleged that an officer or employee was responsible for the disclosure.

Finally, Defendants argue that Plaintiffs' disclosure claim under the Code is actually a failure to safeguard claim, which is not permitted under the Code. Plaintiffs allege that by designing a software application that could be used to access returns and return information online, but failing to secure the system adequately, despite TIGTA warnings, the IRS knowingly or negligently permitted the disclosure of their personal identifying information.

The Court must therefore consider whether Defendants negligently disclosed Plaintiffs' return or return information. Plaintiffs ask the Court to use a "zone of danger" test and accept the allegations that the failure of the IRS to secure the Get Transcript application on the World Wide Web was negligent and the proximate cause of the disclosure of their personal identifying information. Defendants reply that Plaintiffs attempt to present a "failure to protect" claim couched as an "improper disclosure" claim, but the Code does not authorize suit against the IRS based on a failure to protect. Defendants further argue that Plaintiffs' attempt to expand liability under § 7431 to safeguarding claims through a "zone of danger" test would expand the government's waiver of sovereign immunity to include a claim not contemplated by the Code.

There must be a valid waiver of the United States' sovereign immunity before an individual can sue a federal agency. *See Block v. North Dakota*, 461 U.S. 273, 287 (1983) ("The basic rule of federal sovereign immunity is that the United States cannot be sued at all without the consent of Congress."). The principles of sovereign immunity apply equally to federal agencies, officers, and employees acting in their official capacity. *See Fed. Deposit Ins. Corp. v. Meyer*, 510 U.S. 471, 475 (1994); *Kentucky v. Graham*, 473 U.S. 159, 165-66 (1985). This exemption from suit is expressed in jurisdictional terms—that is, federal courts lack subject

matter jurisdiction over suits against the United States in the absence of a clear waiver of sovereign immunity. *See Jackson v. Bush*, 448 F. Supp. 2d 198, 200 (D.D.C. 2006) ("[A] plaintiff must overcome the defense of sovereign immunity in order to establish the jurisdiction necessary to survive a Rule 12(b)(1) motion to dismiss."). Statutes that waive sovereign immunity are strictly construed and any doubt or ambiguity is resolved in favor of immunity. *See Lane v. Pena*, 518 U.S. 187, 192 (1996).

All waivers of sovereign immunity are presumed to be limited. *Cooper*, 132 S. Ct. at 1448 ("Any ambiguities in the statutory language are to be construed in favor of immunity, so that the Government's consent to be sued is never enlarged beyond what a fair reading of the text requires.") (internal citations omitted). Plaintiffs' allegations focus on the alleged negligence of the IRS and the Commissioner in securing the Get Transcript application and failing to comply fully with FISMA and the Modernization Act. In order to address the negligent disclosure theory presented by Plaintiffs, a jury would necessarily first have to determine if the IRS acted negligently by failing to include additional security protections before Get Transcript was made available online.

Plaintiffs' failure to safeguard claim was properly brought under the Privacy Act and not the Code (and dismissed for the reasons stated above). Likewise, Plaintiffs' disclosure claim was properly raised under the Code and not the Privacy Act, because the Code provides a specific cause of action for individuals harmed by improper disclosures by the IRS. Plaintiffs, however, attempt to conflate the two claims and extend the Code to a cause of action for which sovereign immunity has not been waived by forcing the Court and a jury to decide whether the IRS failed to safeguard and then find that that failure was a negligent act that led to disclosure.

The Court reads the text of the Code in favor of immunity and will not extend it to permit Plaintiffs' claim. Plaintiffs' Internal Revenue Code claim (Count 3) will be dismissed.

IV. CONCLUSION

For the reasons stated above, the Court will dismiss all of Ms. DuPree's claims for lack of standing and Mses. Welborn and Windrich's APA claims for lack of standing. Mses. Welborn and Windrich's claims of improper disclosure under the Privacy Act will be dismissed because they are preempted by the Code and their Internal Revenue Act claims will be dismissed for failure to state a claim. The Court will grant Defendants' Motion to Dismiss, Dkt. 24. A memorializing order accompanies this Opinion.

Date: November 2, 2016

/s/
ROSEMARY M. COLLYER
United States District Judge