Nos. 17-5217, 17-5232

In the
United States Court of Appeals
For the
District of Columbia Circuit

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION

Appeal from a Final Judgment of the United States District Court for the District of Columbia in *In re: U.S. Office of Personnel Management Data Security Breach Litigation*, District Court Case No. 1:15-mc-01394-ABJ

CLASS PLAINTIFFS–APPELLANTS' CORRECTED OPENING BRIEF

Daniel C. Girard
Jordan Elias
GIRARD GIBBS LLP
601 California St., 14th Floor
San Francisco, CA 94108
(415) 981-4800

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Ave., N.W.
Washington, D.C. 20036
(202) 220-9600

Counsel for Class Plaintiffs–Appellants

[Additional counsel listed on signature page]

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

RULES

REGULATIONS

OTHER AUTHORITIES

INTRODUCTION

This case involves one of the most troubling data breaches ever—the intrusion into the electronic systems of the United States Office of Personnel Management ("OPM"), which exposed the private information of more than 21 million current and former federal workers. The stolen information includes not only social security numbers and birthdates, but also information of the utmost sensitivity like HIV status, fingerprints, psychiatric health records, and personal histories of alcohol and drug abuse, gambling compulsions, marital discord, and past sexual partners.

After cases arising from this incident were consolidated in D.C. federal court, the government and its security contractor moved to dismiss. The district court dismissed all the claims, without leave to amend, for lack of standing. This was error. The district court's conclusion that it is *implausible* that Plaintiffs are subject to a substantial risk of identity theft is irreconcilable with the government's own decision to devote tens of millions of dollars to protecting the identities of the breach victims. In fact, several Plaintiffs suffered concrete forms of identity theft, such as stolen tax refunds, committed with the very information that was hacked. A range of other injuries Plaintiffs experienced—including understandable distress—resulted from Defendants' deficient data security and independently establish standing. Under this Court's *Attias v. Carefirst* precedent, Plaintiffs

unquestionably have standing to bring their claims. The district court looked outside the complaint to hold otherwise, relying on hearsay that the Chinese government may have carried out these attacks and reasoning that this somehow meant Plaintiffs were not injured. Given Defendants' facial challenge, the district court erred by failing to confine itself to the complaint's four corners.

Plaintiffs alleged that the negligent security measures of OPM's contractor, KeyPoint Government Solutions, Inc. ("KeyPoint"), opened the gates to the wider government network. But the district court erroneously held KeyPoint immune from suit based upon the government's own immunity. Reversal is required because immunity does not shield a contractor who failed to implement the most basic data security measures.

The district court also dismissed the Privacy Act claim, but erred by ignoring Plaintiffs' out-of-pocket losses from actual identity theft, as well as their lost time and expenditures to protect themselves from identity thieves. Both the extremely sensitive nature of the information taken, and the government's own remedial offers, demonstrate that Plaintiffs reasonably spent money to protect their identities.

The district court's dismissal should be reversed.

JURISDICTIONAL STATEMENT

The district court had subject matter jurisdiction over the Privacy Act claim under 28 U.S.C. §1331 and 5 U.S.C. §552a(g)(1) and over the Fair Credit Reporting Act ("FCRA") claim under 28 U.S.C. §1331. The court also had subject matter jurisdiction over the claims against KeyPoint under 28 U.S.C. §1332(d).

The district court entered a final order dismissing all claims on September 19, 2017. Joint Appendix ("JA") 388. Plaintiffs noticed a timely appeal. JA465–70. This Court has jurisdiction under 28 U.S.C. §1291.[1]

ISSUES PRESENTED

1. Did the district court err by holding that Plaintiffs lack standing to assert their claims?

2. Did the district court err by alternatively holding that KeyPoint is protected by derivative sovereign immunity?

3. Did the district court err by alternatively holding that Plaintiffs failed to state a Privacy Act claim?

[1] Plaintiffs brought a breach of contract claim against OPM under 28 U.S.C. §1346, but this appeal does not fall within 28 U.S.C. §1295(a)(2)'s grant of exclusive appellate jurisdiction to the Federal Circuit because the district court determined that it lacked subject matter jurisdiction over the contract claim. Plaintiffs have not appealed that determination. In an abundance of caution, however, Plaintiffs noticed an additional, protective appeal to the Federal Circuit for the sole purpose of preserving their appellate rights in the event this Court concludes that jurisdiction over this appeal lies exclusively in the Federal Circuit. JA471–74. In December 2017, the Federal Circuit stayed that appeal pending resolution of the present appeal.

STATEMENT OF THE CASE

As alleged in the Consolidated Amended Complaint ("CAC"), Defendants did not establish legally required safeguards to ensure the security of personal information of current, former, and prospective employees of the federal government and its contractors. Plaintiffs are a union and 38 individuals who alleged they were harmed by Defendants' failure to safeguard their information and seek relief on behalf of the people whose information was exposed in the breaches of Defendants' electronic systems (the "Data Breaches").

The CAC alleges that OPM's failure to keep their private information secure, despite repeated official warnings of cyber threats and major security lapses in its systems, constitutes willful misconduct in violation of the Privacy Act. The CAC further alleges that KeyPoint's actions and inaction constitute negligence, invasion of privacy, breach of contract, and statutory violations. Plaintiffs seek damages for their resulting injuries.

A. Defendants' Inadequate Data Security

OPM oversees more than two million federal background and security clearance investigations annually, and it contracts with KeyPoint to perform the majority of its investigative work in the field. JA59–61, 63 (CAC ¶¶52–53, 60, 75). OPM collects and maintains—and KeyPoint has access to—millions of personnel files that include names, birthdates, social security numbers, fingerprint

records, and detailed personal, medical, financial, and associational histories. JA61, 63–64, 73–74, 76–78 (CAC ¶¶61, 76, 129, 140, 144). OPM and KeyPoint promised federal employees, contractors, and job applicants that the confidentiality of their personal information would be preserved. JA62, 64 (CAC ¶¶68–70, 77).

The Office of Inspector General ("IG") conducts annual audits of OPM's information security to test and ensure compliance with federal requirements. JA65 (CAC ¶84). In each audit from 2007 to 2015, the IG found that OPM's information security practices suffered from *significant, material deficiencies posing an immediate security threat*. JA66 (CAC ¶¶86–89). OPM controlled numerous electronic systems without valid authorizations, failed to implement multi-factor authentication for accessing systems, failed to patch, segment, and continuously monitor systems, and failed to implement centralized data security protocols. JA66–71 (CAC ¶¶90–113).

OPM repeatedly failed to remedy these problems. In November 2014 the IG advised OPM to shut down all systems lacking current and valid authorizations. *OPM nevertheless kept operating the inadequately secured systems*. JA70 (CAC ¶¶103–04).

B. The Cyberattacks on KeyPoint and OPM

On November 1, 2013, hackers infiltrated OPM's network and stole documents showing how OPM's systems were structured. JA73 (CAC ¶125).

Several weeks later, in December 2013, hackers used the stolen information to breach KeyPoint's systems. JA37, 71 (CAC ¶¶4–5, 114). KeyPoint, which lacked software logs to track malware entering its systems and data exiting its systems, did not detect this breach for nine months and did not notify the victims for another seven months after that. JA72, 98, 106 (CAC ¶¶117, 120–21, 224, 261). KeyPoint's data security suffered from numerous other shortcomings that left it vulnerable to hacking. JA98 (CAC ¶223 (specifying seven deficiencies)).

Among the information hackers stole in the KeyPoint breach was the personal data of over 48,000 people. JA72 (CAC ¶120). Even after learning of this breach—and despite the interconnected nature of OPM's and KeyPoint's systems—OPM did not end or limit KeyPoint's access to its systems. JA37, 63–64, 72, 96 (CAC ¶¶4, 76, 119, 217). Instead, after learning of the KeyPoint breach, OPM contracted for KeyPoint to perform additional background checks. JA72 (CAC ¶¶116, 119). KeyPoint increased its workforce to accommodate the added workload, but did not increase managerial oversight correspondingly. *Id.*

On May 7, 2014, hackers used stolen KeyPoint credentials to access OPM's network. JA73 (CAC ¶127). They installed malware and extracted the personal information of many millions of people who had undergone federal background checks, along with the personal information of millions of their family members and cohabitants, including names, current and former addresses, birthdates, social

security numbers, 5.6 million sets of fingerprints, "[p]sychological and emotional health information," and personal histories of "past sexual partners," "gambling compulsions, marital troubles, and past illicit drug and alcohol use." JA73, 76–78 (CAC ¶¶127, 140–41, 144). The information was stolen "as a result of KeyPoint's negligence in failing to protect and secure its user log-in credentials." JA99 (CAC ¶228).

OPM announced the Data Breaches in June and July 2015. JA75–76 (CAC ¶¶138–40). OPM then offered free fraud monitoring and identity theft protection services, at a cost of approximately $154 million, to the more than 21 million individuals whose private facts had been taken. JA78–79 (CAC ¶¶148–50). Although the theft of their data puts them at risk for the rest of their lives—"More than a Generation," in the words of the House report the district court cited—OPM's remedial offer was for only 18 months or three years. JA79 (CAC ¶150).

C. Plaintiffs' Injuries in the Wake of the Data Breaches

Soon after KeyPoint's and OPM's systems were breached, Plaintiffs began to experience tangible, harmful instances of fraud and identity theft connected to the personal information that was stolen. Tax returns were fraudulently filed using Plaintiffs' identities, causing them to incur costs and delaying their tax refund payments for months or years. JA40–41, 46–49 (CAC ¶¶14, 24, 26, 28). Loans were fraudulently taken out and credit-card and other accounts fraudulently opened

using Plaintiffs' identities, causing them to lose both money and time. JA44–45, 48–51, 57–58 (CAC ¶¶22, 28, 31, 45, 49). Their personal accounts also incurred unauthorized debits, which they spent time trying to get resolved, not always successfully. JA40, 42–43, 49–51, 53–55, 58–59 (CAC ¶¶13, 19, 29–31, 38, 41, 49, 50). In addition, the identities of Plaintiffs' children were stolen. JA50–51, 58–59 (CAC ¶¶31, 50). Plaintiffs suffered further harms in seeking to mitigate the effects of the Data Breaches by purchasing credit monitoring and repair services, and by devoting extra time to tracking their accounts and credit reports and attempting to remedy the identity theft they experienced. JA40–59 (CAC ¶¶13–22, 25–34, 36–44, 46–50).

D. The District Court's Dismissal Opinion

The district court dismissed Plaintiffs' claims for lack of Article III standing despite acknowledging that several Plaintiffs alleged harm in the form of identity theft or fraudulent account activity, and commenting that "standing is a very close and difficult question in this case." JA440 (Opinion 52). Twenty Plaintiffs suffered identity theft or fraud, including by having false tax returns filed in their names. JA40–44, 46–51, 53–55, 57–59 (CAC ¶¶13–14, 16–17, 19, 21, 24, 26, 28–32, 38–39, 41, 45, 49–50). The district court held that all but two Plaintiffs did not suffer an injury in fact, reasoning in part that the Plaintiffs who had incurred

unauthorized account charges did not affirmatively allege that they were held responsible for those charges. JA421 (Opinion 33).

The district court held that Plaintiffs had not alleged sufficient risk of future harm because there was no indication that hackers stole their personal information for the purpose of stealing their identities. JA428 (Opinion 40). The district court rejected Plaintiffs' allegations that the hack was committed for the purpose of misusing their data, *see* JA72–74 (CAC ¶¶117, 128, 132), opining that the perpetrator may have been the Chinese government. The court wrote that "the state-sponsored nature of the attack" was likely, even absent a public statement from OPM—or any complaint allegation—that the attack was state sponsored. JA431–32 (Opinion 43–44). At oral argument, the government refused to take a position on who perpetrated the hack or whether the Chinese were involved, advising the court not to "pay any attention to any discussion … in the public sphere, about who was behind this breach and what the purpose of the breach was[.]" JA207–09 (10/27/16 Hr'g Tr. 16–18). The court noted in its opinion that Plaintiffs "plausibly alleged that the building blocks of some forms of identity theft—social security numbers coupled with names, birthdates, and addresses—were included in the cache of information that was taken from OPM." JA433 (Opinion 45). But, without allegations of a particularized objective behind the hack, the court wrote that it could not infer the hack was done to commit fraud or

steal identities. JA433–34 (Opinion 45–46). The court also found that Plaintiffs' purchase of credit monitoring to avoid identity theft did not constitute injury in fact because the risk avoided was too speculative, notwithstanding the government's remedial offer. JA435–36 (Opinion 47–48). Consequently, the court held that only the two Plaintiffs who alleged they incurred unreimbursed out-of-pocket costs other than credit monitoring fees had alleged cognizable harm.

The district court then concluded, however, that even those two Plaintiffs lacked standing as they had not alleged facts plausibly showing their injuries were fairly traceable to Defendants' violations. JA436–40 (Opinion 48–52). The court reasoned in part that other data breaches could not be ruled out as the source of the harm. JA439 (Opinion 51). The court did so despite class counsel's representation that the Plaintiffs named in the complaint reported that they had not received notice of being exposed to other data breaches. JA224 (10/27/16 Hr'g Tr. 33).

The district court proceeded to render alternative holdings, including that derivative sovereign immunity barred the claims against KeyPoint. JA459–60 (Opinion 71–72). In addition, mirroring its standing findings, the court found that all but two Plaintiffs failed to plausibly allege that they had sustained actual damages under the Privacy Act. JA441–42 (Opinion 53–54). The court further found that even the two Plaintiffs with "actual damages" lacked viable claims

because they had not plausibly alleged that their injuries resulted from OPM's actions or inaction. JA445–46 (Opinion 57–58).

STANDARD OF REVIEW

De novo review applies to this appeal. *Attias v. Carefirst, Inc.*, 865 F.3d 620, 625 (D.C. Cir. 2017), *cert. denied*, 138 S.Ct. 981 (2018); *Albrecht v. Comm. on Emp. Benefits of Fed. Reserve Emp. Benefits Sys.*, 357 F.3d 62, 65 (D.C. Cir. 2004). Plaintiffs' complaint need only set forth enough facts to state claims that are facially plausible. *Rudder v. Williams*, 666 F.3d 790, 794 (D.C. Cir. 2012). The Court must accept the truth of well-pled allegations, construe them as a whole, and draw all inferences in Plaintiffs' favor. *Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (Rule 12(b)(1)); *Atherton v. D.C. Office of Mayor*, 567 F.3d 672, 677 (D.C. Cir. 2009) (Rule 12(b)(6)).

SUMMARY OF THE ARGUMENT

1. The district court misapplied the Article III standing criteria. In barring the courthouse doors, the court acted directly counter to this Court's teaching that standing erects a "low bar" and "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury." *Attias*, 865 F.3d at 622, 627. Several Plaintiffs here *have* alleged that they suffered actual identity theft—requiring reversal under *Attias*. The theft of their birthdates and social security numbers also exposes Plaintiffs to an ongoing threat

of identity theft. And Plaintiffs alleged that they suffered additional Article III injuries in the form of credit monitoring and other expenditures to mitigate identity theft, as well as lost time and distress. Defendants' alleged statutory violations independently give rise to cognizable harm. All of these alleged injuries are traceable to Defendants' alleged data security deficiencies and are judicially redressable.

2. The district court erred by holding the claims against KeyPoint precluded by derivative sovereign immunity. Derivative sovereign immunity only protects contractors from liability for following specific government directives, and it does not extend to conduct that is negligent or in breach of (or simply left unaddressed by) an agreement with the government. Plaintiffs' complaint enumerates KeyPoint's data security failures and alleges those failures constitute negligence, breached KeyPoint's government contract, and enabled hackers to break into OPM's systems.

3. The district court erred in dismissing the Privacy Act claims against OPM, in light of the economic harm multiple Plaintiffs suffered shortly after the Data Breaches.

ARGUMENT

I. THE DISTRICT COURT ERRED IN HOLDING THAT PLAINTIFFS LACK STANDING TO SUE.

Article III standing requires an injury in fact, traceability, and redressability, and "each element must be supported … with the manner and degree of evidence required at the successive stages of the litigation." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (citations omitted). There is a "low bar to establish[ing] … standing at the pleading stage." *Attias*, 865 F.3d at 622.

A. Plaintiffs' Allegations Meet Article III's Injury-in-Fact Requirement.

"At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice." *Lujan*, 504 U.S. at 561. Hence "[t]he injury-in-fact requirement is 'very generous' to claimants, demanding only that the claimant 'allege[] some specific, "identifiable trifle" of injury.'" *Cottrell v. Alcon Labs.*, 874 F.3d 154, 162 (3d Cir. 2017) (citations omitted).

1. *Future Harm*: Plaintiffs Sufficiently Alleged Injury Based on a Substantial Risk of Identity Theft.

The district court's cramped view of standing is incompatible with this Court's decision in *Attias*. There, this Court held that plaintiffs' allegations that their private information had been disclosed in a data breach satisfied Article III's injury-in-fact requirement. The plaintiffs alleged that the breach resulted from the defendants' negligence, "and that the data 'accessed on Defendants' servers'

place[d] plaintiffs at a high risk of financial fraud." 865 F.3d at 628. This Court agreed, citing "experience and common sense" to conclude that the alleged risk was at least "substantial": "[P]ortions of the complaint would make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identity fraud, even if"—unlike what happened here—"their social security numbers were never exposed to the data thief." *Id.*

a. The District Court Relied on Inapposite Case Law Instead of *Attias*.

Although this Court issued *Attias* before the decision below was rendered, the district court did not apply its clear teaching. The information taken in this case includes not only social security numbers but information even more sensitive, such as psychiatric records and fingerprints. Disregarding *Attias* and the Supreme Court law the Court applied in that case, the district court below perceived "no controlling authority on whether plaintiffs alleging actual harm must allege economic losses from a data breach to show injury in fact." JA423 (Opinion 35). *Attias* squarely answered this question, but the district court instead followed inapposite, unpublished decisions from other circuits to hold that "plaintiffs in a data breach case must allege not only that their personal data was misused, but also that they suffered economic loss as a result." JA422 (Opinion 34). The court then improperly brushed aside Plaintiffs' allegations of lost money and time attributable to the Data Breaches to find insufficient allegations of economic loss.

The district court's reasoning is incompatible with this Court's holding in *Attias* that the unauthorized taking of social security numbers—and here, an additional vast array of exceedingly sensitive information—*does* create a threat of identity theft sufficient to confer Article III standing. The facts alleged in Plaintiffs' complaint demonstrate a serious risk of harm that even the government recognized when it offered the victims credit monitoring. JA79 (CAC ¶150). "It is unlikely that [the government] did so because the risk is so ephemeral that it can safely be disregarded." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015).

The district court premised its holding that data breach plaintiffs lack standing absent "economic loss" upon the Second Circuit's unpublished, non-binding opinion in *Whalen v. Michael Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017), a case that, unlike ours, did not involve the theft of social security numbers. *Whalen* is inapposite:

> The plaintiff in *Whalen* alleged that her credit card information was stolen in a data breach, and … subsequently "physically presented for payment" in Ecuador on two occasions. However, …. Whalen never alleged that fraudulent charges were actually incurred on her credit card, she never alleged a plausible threat of future fraud "because her stolen credit card was promptly cancelled," and Whalen did not allege that any other information—such as her birth date or Social Security number—was taken in the breach. Moreover, Whalen did not allege "any time or effort that she herself has spent monitoring her credit." Thus, the Second Circuit held that Whalen did not adequately allege that the data breach caused Whalen to suffer any injury that was concrete and particularized.

In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *15 (N.D. Cal. Aug. 30, 2017) (citations omitted).

Plaintiffs' injury allegations in this case go far beyond attempted misuse of a single, already-cancelled credit card. Among other things, Plaintiffs alleged a host of actual economic injuries suffered when the same information compromised in the Data Breaches (birthdates, addresses, and social security numbers) was used to perpetrate identity fraud. *E.g.*, JA40–41, 44, 46–48, 50–51 (CAC ¶¶14, 21, 24, 26, 28, 31, 32 (seven Plaintiffs had fraudulent tax returns filed in their names, resulting in delayed payment of their tax refunds)).

The out-of-circuit district court cases cited by the district court below offer no better support for its holding that data breach plaintiffs must have already experienced economic harm to have standing. In *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013), the district court read *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), as standing for the proposition that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing." But in *Remijas*, the Seventh Circuit held that "allegations of future injury are sufficient to survive a 12(b)(1) motion" in a data breach case. The court explained that "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such

an injury will occur." 794 F.3d at 693–94 (citing *Clapper*). This intervening appellate authority required the district court in *Barnes & Noble* to "conclude[] that the complaint alleges injury." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). The superseded *Barnes & Noble* order relied upon below also conflicts with this Court's recognition in *Attias* that both *Clapper* and subsequent Supreme Court decisions hold that a "substantial risk" of harm may suffice. *Attias*, 865 F.3d at 626–27 (citing, *inter alia*, *Susan B. Anthony List v. Driehaus*, 134 S.Ct. 2334, 2341 (2014)); *see also, e.g.*, *In re Zappos.com, Inc.*, No. 16-16860, — F.3d —, 2018 WL 1883212, at *2–3 (9th Cir. Apr. 20, 2018) (holding that standing in a data breach case may be based on "the risk of identity theft," and reversing dismissal of claims of plaintiffs who had not suffered financial fraud).

Attempting to distinguish *Attias* and other decisions holding that a substantial risk of identity theft creates Article III standing, the district court reasoned that "[t]he hackers' goal has not been revealed" and the complaint "does not point to any particular objective behind the breach" beyond "improper use" of the hacked data. JA433 (Opinion 45 & n.21). The district court, then, would require data breach plaintiffs, subject to Rule 11, to itemize the specific "objective[s]" of unknown criminals when, "at the very least, it is plausible … to infer that [they have] the intent and the ability to use that data for ill." *Attias*, 865 F.3d at 628.

A data breach need not have been motivated by a specific "purpose" to commit fraud or identity theft for the stolen information to find its way to the black market. Nor need there be any such nefarious purpose for Plaintiffs reasonably to spend money and time protecting their identities. Thieves don't steal people's personally identifiable information to send them Hallmark cards.

The district court's further efforts to distinguish *Attias*, as involving stolen credit-card information, *see* JA428, 434 (Opinion 40, 46), further undermine its conclusion. Not only may fraudulent payment-card charges be reimbursed in whole or in part, *see Remijas*, 794 F.3d at 697, but payment-card data is itself readily changeable: new cards simply need to be issued, eliminating the risk of future harm. By contrast, what was stolen here—the most personal and sensitive data imaginable, such as family member names and birthdates, current and past residences, and health, employment, and educational records, as well as candid personal histories of addictions and adultery—can never be undone.

b. The District Court Improperly Drew Inferences Against Plaintiffs Based on Extra-Complaint Material, Including Inadmissible Hearsay.

Plaintiffs adequately alleged an impending threat of identity theft based on the nature of the stolen information and the tax fraud, unauthorized account openings, and other identity theft incidents they experienced. But instead of

accepting Plaintiffs' factual allegations as true, the district court supplied its own theory of the hack based on extraneous material.

The district court sought to distinguish *Attias* by referencing a House report and news accounts suggesting the Chinese government carried out the Data Breaches for political reasons. JA431–33 (Opinion 43–45). None of this material supported the court's finding that Plaintiffs did not suffer economic harm plausibly caused by the Data Breaches, or that they do not face a substantial risk of such harm going forward.

The cited House report nowhere suggests that victims need not fear economic harm or that Chinese hackers would not offer up the information for sale on the black market or use it to commit fraud. In fact, the House report includes a statement of former CIA Director Michael Hayden that the personnel database "remains a treasure trove of information that is available to the Chinese until the people represented by the information age off."[2] The report also identifies "two threat actor groups" as the likely culprits,[3] and a report from information security expert Brian Krebs—which the district court did *not* cite—found that these "same

[2] https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf at iii.

[3] *Id*. at 157–58.

Chinese hackers also have been *selling access* to compromised computers within [Fortune 500] companies to help perpetrate future breaches."[4]

That a cyberattack may be "state sponsored" does not protect the victims from harm. The massive Yahoo data breaches have been linked to Russian state-sponsored actors,[5] yet DOJ acknowledged that consumer information from those breaches has been exploited for financial gain.[6] Similarly, although the FBI confirmed that North Korea hacked Sony in retaliation for the movie "The Interview," the employees whose private information was stolen had standing because of the "credible threat of real and immediate harm[.]" *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600-RGK, 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2015). Put simply, the district court's conclusion that victims of these Data Breaches need not fear identity theft defies "experience and common sense." *Attias*, 865 F.3d at 628.

Moreover, the court's selective reliance on news accounts and a House report was improper. Like the defendant in *Zappos*, the district court below "rel[ied] on facts outside the Complaint[] (or contentions about the absence of

[4] https://krebsonsecurity.com/tag/deep-panda/ (emphasis added).

[5] https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

[6] *Id*. (a defendant "also exploited his access to Yahoo's network for his personal financial gain").

certain facts), which makes its argument one that may be appropriate for summary judgment but not one that may support a facial challenge to standing at the motion to dismiss stage." *Zappos*, 2018 WL 1883212, at *6.

The government in this case represented that its standing challenge was facial, not factual, and it implored the district court to *ignore* public discussion about the identity of the hackers. JA206–09 (10/27/16 Hr'g Tr. 15–18). Therefore, the court could not consider material beyond the confines of the complaint. *See McGary v. Hessler-Radelet*, 156 F.Supp.3d 28, 32 (D.D.C. 2016) ("[A] facial challenge is confined to the four corners of the complaint"). The district court should have limited itself to material "incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). Yet the court accepted the truth of hearsay in news accounts that would have been inadmissible even at a later stage, *see Atkins v. Fischer*, 232 F.R.D. 116, 132 (D.D.C. 2005), and in doing so drew inferences *against* the pleading party. And congressional reports, as the government conceded below, are "not of the sufficient reliability to use[.]" JA208 (10/27/16 Hr'g Tr. 17).

The only other sources the district court cited in its China discussion were pre-MDL pleadings that the master CAC superseded. *See* JA421 (Opinion 43 & n.20) (conceding "this ruling is not based on the original complaints that were

consolidated and amended in this multidistrict litigation"); *Gelboim v. Bank of Am. Corp.*, 135 S.Ct. 897, 904 n.3 (2015). Thus, the district court was not empowered to dismiss the CAC on the basis of the cited materials. While it acknowledged that "a finding concerning the source of the breach is beyond the scope of this proceeding at this juncture," JA432–33 (Opinion 44–45), the court effectively made just such a finding.

2. *Past Harm*: Plaintiffs Sufficiently Alleged Injury Based on Economic Loss.

The district court also incorrectly concluded that all but two Plaintiffs had not adequately alleged economic harm from the Data Breaches. One need only read the complaint to see otherwise.

a. Many Plaintiffs Experienced Identity Fraud Committed with the Same Information That Was Taken.

In *Attias*, this Court held that plaintiffs who "allege[d] the theft of social security [and] credit card numbers" pleaded injury in fact sufficient to seek relief from the insurer that maintained this information but failed to protect it. 865 F.3d at 627. Likewise, Plaintiffs in this case alleged that social security numbers were among the personal details stolen, and define "sensitive personal information" (used throughout the complaint) to include, "at a minimum, Social Security numbers and birthdates." JA36, 39, 77–78 (CAC ¶¶1, 10, 144).

Criminals can use social security numbers in tandem with names, addresses, and birthdates to open bank accounts, take out loans, steal tax refunds, and commit other crimes in Plaintiffs' names. *See, e.g.*, *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 32 (D.D.C. 2014) (noting that to open an unauthorized account or take out an unauthorized loan, "one would likely need a person's name, address, date of birth, and social security number—exactly the sort of information" stolen in this case). As in *Attias*, the loss of such information exposed and continues to expose Plaintiffs to serious harm.

Many Plaintiffs experienced identity theft from misuse of their social security numbers following the Data Breaches. *E.g.*, JA40–42, 44–51, 54–55 (CAC ¶¶14 (fraudulent tax return filed), 17 (social security fraud attempted), 21 (fraudulent tax return filed), 22 (twelve accounts fraudulently opened in Plaintiff's name and in collections), 24 (fraudulent tax return filed), 26 (fraudulent tax return filed), 28 (fraudulent tax return filed), 31 (fraudulent tax return filed), 32 (fraudulent tax return filed), 41 (utility fraud committed using social security number)).

These same Plaintiffs alleged that these incidents caused concrete and particularized economic damage. *Id.* (CAC ¶¶14 (tax refunds delayed), 17 (Plaintiff had "to spend time verifying his identity and creating an identity theft profile with the Social Security Administration"), 21 (Plaintiff "incur[red] $30.95

per month in fees to make payments" and spent "many hours attempting to resolve these tax fraud issues"), 22 (Plaintiff required to pay $198 to a credit repair firm, $50 to obtain copies of her credit report, and "spent between 40 and 50 hours dealing with the fraudulent accounts"), 24 (tax refunds delayed), 26 (tax refunds delayed), 28 (Plaintiff "has not yet received her federal or state income tax refunds," and various fraudulent loans were taken out in her name and placed in collections, requiring "over 50 hours"), 31 (account fraudulently opened in Plaintiff's name "had an outstanding balance of almost $3,000" and "remains under investigation"), 32 (tax refunds delayed), 41 (fraudulently opened account incurred charges)).

Plaintiffs accordingly alleged that these incidents resulted in concrete harm. As this Court has recognized, "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury." *Attias*, 865 F.3d at 627; *see also id.* at 626 n.2 (plaintiffs who "claimed that their anticipated tax refund had gone missing" had demonstrated injury in fact for standing purposes).

Contrary to the district court's reasoning, *see* JA423 (Opinion 35), Plaintiffs need not allege that they were never reimbursed for their lost time and money, including lost interest from delayed tax refund payments. Reimbursement from financial institutions "defeats neither injury-in-fact nor redressability" because "a

favorable judicial decision could redress any injuries caused by less than full reimbursement of unauthorized charges." *Remijas*, 794 F.3d at 697. Plaintiffs also "have standing because … unauthorized withdrawals from their accounts cause a loss (the time value of money) even when banks later restore the principal[.]" *Barnes & Noble*, 887 F.3d at 828. Thus, the possibility that some Plaintiffs were or may be reimbursed for their losses would not change the fact that they *already* suffered actual injuries—which occurred and were complete at the point of loss. *See In re Nexium Antitrust Litig.*, 777 F.3d 9, 27 (1st Cir. 2015) ("In contemplation of law the claim for damages arose at the time the extra charge was paid. Neither the fact of subsequent reimbursement … nor the disposition which may hereafter be made of the damages recovered is of any concern to the wrongdoers.") (citing *Adams v. Mills*, 286 U.S. 397, 407 (1932)).

b. Plaintiffs Spent Money Responding to Identity Theft Incidents and Paying for Credit Monitoring After the Data Breaches.

Plaintiffs' reasonable "out-of-pocket mitigation expenses are also sufficient to allege injury in fact[.]" *Yahoo*, 2017 WL 3727318, at *16; *see also Attias*, 865 F.3d at 629. Plaintiff Jane Doe,[7] for example, had twelve unknown accounts fraudulently opened in her name and placed in collection for nonpayment. JA44–45 (CAC ¶22). In response, she paid approximately $198 to a firm that assisted her

[7] Several Plaintiffs used pseudonyms out of concern for their personal safety.

in closing these accounts and removing them from her credit history. *Id*. Plaintiff Charlene Oliver received a letter from her electricity company stating that her utility account had been closed, was no longer in her name, and had incurred charges of $500. JA54–55 (CAC ¶41). The electricity company purported to refund her deposit by sending a check made out to another individual, and demanded that she pay an additional $390 to restore service. This dispute remains unresolved and Oliver pays $100 each month to a firm to restore her credit. *Id*.

As noted above, OPM offered free fraud monitoring and identity theft protection services to the people whose private facts were stolen. JA78–79 (CAC ¶¶148–50). OPM also referred the victims to a government website recommending that data breach victims "purchase a credit freeze to ensure that no one can pull or modify a credit report," which "typically costs between $5 and $15." JA79 (CAC ¶151). OPM's conduct shows that Plaintiffs' out-of-pocket payments for similar services after the Data Breaches were reasonable.

For example, Plaintiff John Doe II pays $329 annually, and Plaintiff Paul Daly pays $29.95 each month, for credit monitoring to guard against identity theft. JA44, 46–47 (CAC ¶¶21, 25). These costs, incurred because of a data breach, are concrete injuries. *See, e.g.*, *Remijas*, 794 F.3d at 694 (credit monitoring costs "easily" qualified as Article III injury); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164–65 (1st Cir. 2011); *Sony Pictures*, 2015 WL 3916744, at *4–5.

The district court refused to presume a reasonable concern about identity theft because the court's own research, *see* JA207 (10/27/16 Hr'g Tr. 16), disclosed extra-complaint material identifying China as the "likely source of the hacking." JA432 (Opinion 44). Yet, even assuming that material was properly considered, reports of Chinese involvement did not surface for some time, *id*., and a conclusion that Plaintiffs did not reasonably incur costs to protect themselves from identity theft is at odds with the actual identity theft incidents set out in the complaint and the extremely sensitive nature of the hacked information.

Plaintiffs' need to monitor their credit is not eliminated if Chinese hackers, rather than others, were the ones who stole their social security numbers and other sensitive facts. Because it was reasonable for Plaintiffs to take steps to protect themselves from identity theft, their self-protection expenditures confer standing:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken. That risk is much more substantial than the risk presented to the *Clapper* Court, and satisfies the requirement of an injury in fact.

Attias, 865 F.3d at 629.

c. Plaintiffs Lost Time as a Result of the Data Breaches.

"[T]he value of one's own time needed to set things straight is a loss from an opportunity-cost perspective." *Barnes & Noble*, 887 F.3d at 828. Therefore, the

"time and effort" a data breach victim reasonably expends in "monitoring both his card statements and his other financial information" gives rise to standing. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965–69 (7th Cir. 2016); *see also In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016).

Plaintiffs devoted considerable time to closing fraudulent accounts and repairing damage to their credit after the Data Breaches. *E.g.*, JA40, 42–45, 54 (CAC ¶¶13 (ten hours communicating with bank and many more hours disputing fraudulent credit inquiries), 19 (ten hours communicating with bank and reviewing and submitting affidavits), 22 (between 40 and 50 hours dealing with fraudulent accounts, communicating with the FBI, and attempting to gain access to credit report), 39 (many hours attempting to resolve identity fraud). In addition, many Plaintiffs spend more time monitoring their credit now than before the Data Breaches. *E.g.*, JA46–52 (CAC ¶¶25–33). Their lost time has value, and is an injury in fact.

3. *Past, Present, and Future Harm*: Plaintiffs Sufficiently Alleged Injury Based on Their Distress and the Invasion of Their Privacy.

"Although tangible injuries are perhaps easier to recognize, [the Supreme Court has] confirmed … that intangible injuries can nevertheless be concrete."

Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1549 (2016). Distress and invasion of privacy are two cognizable, intangible injuries present here.

First, mental or emotional distress caused by a data breach constitutes injury in fact. *See In re Dep't of Veterans Affairs (VA) Data Theft Litig.*, Misc. Action No. 06-0506 (JR), 2007 WL 7621261, at *3 (D.D.C. Nov. 16, 2007); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010). Several Plaintiffs in this case alleged that the Data Breaches caused them distress. *E.g.*, JA42–43 (CAC ¶¶18–19).

Second, "invasion of privacy" from the disclosure of private information can be a "concrete injury." *Owner-Operator Indep. Drivers Assoc. v. DOT*, 879 F.3d 339, 343 (D.C. Cir. 2018). Invasion of privacy is "a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1340–41 (11th Cir. 2017), and the release of Plaintiffs' personal information via the Data Breaches invaded their privacy. *See, e.g.*, *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 34 (2d Cir. 2017).

4. *Statutory Harm*: Plaintiffs Sufficiently Alleged Injury Based on Defendants' Violations of Federal Privacy Statutes.

a. OPM's Privacy Act Violations and KeyPoint's FCRA Violations Resulted in Invasions of Plaintiffs' Privacy.

Similarly, Defendants' alleged statutory violations demonstrate injury in fact because they caused an invasion of Plaintiffs' statutorily-protected privacy rights.

JA87–89, 102–04 (CAC ¶¶175–85, 245–52). In *Spokeo*, the Supreme Court held that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact" and "a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." 136 S.Ct. at 1549 (emphasis in original).

First, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id.* Second, Congress "may elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Id.* (alteration in original) (citation omitted). Both historical practice and congressional action show that Defendants' statutory violations constitute injuries in fact because they caused Plaintiffs' privacy to be invaded.

"[T]he common law … encompass[ed] the individual's control of information concerning his or her person." *DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989). The tort of intrusion upon seclusion has long held liable "[o]ne who intentionally intrudes, physically or otherwise, upon … [another's] private affairs or concerns … if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS §652B (1977). "The intrusion itself makes the defendant subject to liability, even though

there is no publication or other use of any kind of the [private information]." *Id.*, cmt. b. Further, a defendant "may be liable for a *third party's* intrusion where the defendant 'furnished means and opportunities' for the intrusion." DAVID A. ELDER, PRIVACY TORTS §2:9 (2017) (emphasis added). This long-established tort is "well nigh conclusive" in showing that disputes over alleged privacy invasions are "cases and controversies of the sort traditionally amenable to, and resolved by, the judicial process." *Sprint Commc'ns Co., L.P. v. APCC Servs., Inc.*, 554 U.S. 269, 285 (2008).

The Privacy Act and FCRA also reflect Congress's judgment that invasions of privacy should be "elevat[ed] to the status of legally cognizable injuries." *Spokeo*, 136 S.Ct. at 1549. With the Privacy Act, Congress recognized that "the right to privacy is a personal and fundamental right" and that "the increasing use of computers and sophisticated information technology … has greatly magnified the harm to individual privacy that can occur[.]" Pub. L. No. 93-579, §§2(a)(4), 2(a)(2), 88 Stat. 1896 (1974). Congress declared that "[t]he purpose of [the Privacy] Act is to provide certain safeguards for an individual against an invasion of personal privacy" by requiring agencies to adopt "adequate safeguards … to prevent misuse of [identifiable personal] information." *Id.* §2(b). Thus, 5 U.S.C. §§552a(b) and 552(e)(10) regulate when and how such information can be disclosed and the safeguards that must be put in place to maintain its security, and

Section 552a(g) makes violations of these sections actionable. These provisions embody Congress's elevation of the intangible harm of invasion of privacy to a statutorily-recognized injury. *See Parks v. IRS*, 618 F.2d 677, 683 (10th Cir. 1980).

Congress made a similar judgment with FCRA. It found that "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with … a respect for the consumer's right to privacy," Pub. L. No. 91-508, §602(a)(4), 84 Stat. 1114 (1970), and it declared that "the purpose of this [Act is] to require that consumer reporting agencies adopt reasonable procedures … with regard to the confidentiality … of such [credit] information[.]" *Id.* §602(b). To these ends, 15 U.S.C. §1681b(a) prohibits furnishing consumer reports without a statutorily-permitted purpose, while Section 1681e(a) requires credit reporting agencies to "maintain reasonable procedures designed to" prevent violations of Section 1681b(a). And Congress created a private right of action with Sections 1681n and 1681o.

Accordingly, "[j]ust as the common law permitted suit in such instances," where, as here, alleged Privacy Act or FCRA violations brought about the very harm Congress sought to prevent, the violations give rise to Article III injuries. *Spokeo*, 136 S.Ct. at 1549.

b. The District Court's Reasoning as to Standing Based on Statutory Violations Is Incorrect.

None of the district court's reasons for rejecting standing based on Defendants' alleged statutory violations is correct. First, it believed that it could not find standing given an "absence of authority to support Plaintiffs' proposal[.]" JA409 (Opinion 21). But as shown above, *Spokeo* supports Plaintiffs' standing to pursue their Privacy Act and FCRA claims because they alleged the unauthorized exposure of their highly sensitive data.

Recent decisions by this Court and other Courts of Appeals confirm Plaintiffs' standing to pursue these claims. In *Owner-Operator Independent Drivers Association*, standing existed based upon the federal government's disclosure of inaccurate information about two truck drivers. 879 F.3d at 344–45. In *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, customers whose sensitive private information had been hacked alleged that the defendant violated FCRA by failing to safeguard the information. 846 F.3d 625 (3d Cir. 2017). Applying *Spokeo*'s two-part test, the Third Circuit first observed that unauthorized disclosure of information has "long been seen as injurious." *Id.* at 638. Indeed, "improper dissemination of information can itself constitute a cognizable injury" even "without proving actual damages." *Id.* at 638–39; *see also id.* at 642 (Schwartz, J., concurring in the judgment).

Moving to *Spokeo*'s second prong, the Third Circuit observed that "with the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself." *Id.* at 639. And because "the intangible harm that FCRA seeks to remedy has a close relationship to a harm [i.e. invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," the court had "no trouble concluding that Congress properly defined an injury that give[s] rise to a case or controversy where none existed before." *Id.* at 639–40 (alterations in original) (quotation marks and citation omitted); *accord Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1114–16 (9th Cir. 2017) (on remand, recognizing long history of protecting "reputational and privacy interests" and holding that FCRA was enacted to protect those interests), *cert. denied*, 138 S.Ct. 931 (2018).

Second, the district court thought that holding that Defendants' statutory violations produce cognizable harm "would collapse" the three components of standing analysis—injury, traceability, and redressability—into "a single allegation: my data was involved." JA412–13 (Opinion 24–25). That is incorrect. A data breach plaintiff still must plausibly allege that the harm is fairly traceable to the defendant's alleged violations and is redressable in court. OPM and KeyPoint violated the statutes—nobody else—and damages can redress intangible injuries like invasions of privacy. *See* RESTATEMENT (SECOND) OF TORTS §652H (1977).

Third, the district court interpreted *Spokeo* as requiring a showing of some sort of harm—even intangible harm—accompanying the statutory violation, and the court saw no such harm present here. JA415–20 (Opinion 27–32). But, because Plaintiffs' personal information was disclosed in the Data Breaches, they have suffered an invasion of privacy—which *is* an intangible harm beyond the statutory violation.

Fourth, the district court stated that recognizing Plaintiffs' standing would be "hollow" given its finding that their Privacy Act claim was inadequately pleaded. JA419 (Opinion 31). Whether Plaintiffs state a claim is, of course, a merits question separate from standing, *see Horizon Healthcare*, 846 F.3d at 633 n.9, and courts "must therefore assume that on the merits the plaintiffs would be successful in their claims" when determining standing. *In re Navy Chaplaincy*, 534 F.3d 756, 760 (D.C. Cir. 2008); *Attias*, 865 F.3d at 629.

In sum, Plaintiffs alleged that Defendants' violations of the Privacy Act and FCRA resulted in intangible harm of precisely the kind these statutes were enacted to prevent—invasion of privacy—and that American courts have traditionally had the power to redress. Therefore, under *Spokeo*, Plaintiffs have standing to pursue their Privacy Act and FCRA claims.

* * *

As shown in the above discussion, Plaintiffs have alleged sufficient facts to demonstrate their injuries in fact consisting of past, present, and future harm.

B. Plaintiffs' Allegations Meet Article III's Traceability Requirement.

The second prong of Article III standing—traceability—requires plausible allegations of a causal link between the alleged injury in fact and the alleged violations. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998). As this Court held in the data breach setting:

> It is of course true that the thief would be the most immediate cause of plaintiffs' injuries, should they occur, and that [defendant's] failure to secure its customers' data would be one step removed in the causal chain. But Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be "fairly traceable" to the defendant.

Attias, 865 F.3d at 629; *see also Edmonson v. Lincoln Nat'l Life Ins. Co.*, 725 F.3d 406, 418 (3d Cir. 2013) (the "fairly traceable" requirement can be met "even where the conduct in question might not have been a proximate cause of the harm, due to intervening events.") (citation omitted); *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003) ("Importantly … we are concerned with something less than the concept of 'proximate cause.'").

Here, Plaintiffs alleged that Defendants failed to secure their sensitive personal information, JA64–73 (CAC ¶¶78–124); that this information was stolen

by hackers who gained access to Defendants' inadequately secured computer systems, JA71–78 (CAC ¶¶114–37, 143–47); and that Plaintiffs have consequently been subjected to actual and imminent harm. JA40–59, 81–83 (CAC ¶¶13–50, 163). No more is required at this stage to allege that the harm is plausibly traceable to Defendants' alleged violations. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (allegations that laptops containing personal information were not adequately secured and then were stolen, and that plaintiffs subsequently had their identities stolen, satisfied Article III); *Zappos*, 2018 WL 1883212, at *7 (risk of identity theft following data breach was plausibly traceable to that breach despite existence of other breaches that might have compromised the same information).

1. The District Court Erred by Rejecting Plaintiffs' Allegations That the Harm Resulted from These Breaches.

Even the district court acknowledged that Jane Doe's and Charlene Oliver's allegations of out-of-pocket loss sufficiently plead injury in fact. JA436 (Opinion 48). But the court went on to hold that these two Plaintiffs lack standing on the ground that, given the occurrences of *other* data breaches, Plaintiffs cannot "plausibly allege[] any connection between the OPM breaches and the claimed harm." *Id*. The court so held despite Plaintiffs' allegations that "[a]s a result of *Defendants'* violations of law, Plaintiffs and Class members have sustained and will continue to sustain economic loss and other harm," and despite class counsel's

representation that the Plaintiffs reported not being notified of exposure to other data breaches. JA81, 224 (CAC ¶163 (emphasis added); 10/27/16 Hr'g Tr. 33).

Regardless, that another data breach "might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach" at issue. *Remijas*, 794 F.3d at 696. If multiple breaches "could have exposed the plaintiffs' private information to the hackers, then 'the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the "but-for" cause of the plaintiff's injury.'" *Id.* (quoting *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring)). Furthermore, "to allow Defendants to rely on other data breaches to defeat a causal connection would 'create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.'" *Yahoo*, 2017 WL 3727318, at *19 (quoting *In re Anthem, Inc. Data Breach Litig.*, 162 F.Supp.3d 953, 988 (N.D. Cal. 2016)).

Plaintiffs should not be required to negate other potential causes of harm before taking discovery: "That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from

[defendant]), is less about standing and more about the merits of causation and damages." *Zappos*, 2018 WL 1883212, at *7.

2. The District Court Erred by Drawing Adverse Inferences from Plaintiffs' Allegations of Identity Theft.

Under controlling precedent, the district court should have "assume[d], for purposes of the standing analysis, that plaintiffs will prevail on the merits of their claim that [Defendants] failed to properly secure their data and thereby subjected them to a substantial risk of identity theft"—leaving "little difficulty [in] concluding that their injury in fact is fairly traceable to [Defendants]." *Attias*, 865 F.3d at 629. Instead, the district court attempted to downplay the identity theft incidents Plaintiffs experienced as being "separated across time and geography," and "follow[ing] no discernible pattern." JA439 (Opinion 51). The court thereby presumed that fraud resulting from a data breach necessarily follows a particular "pattern," with incidents occurring at the same time and in the same locale. There is no basis for that presumption. Nor is it correct.

The district court further reasoned that the account fraud Plaintiffs experienced could not have been directly committed with the information taken in the Data Breaches. JA429–30, 439–40 (Opinion 41–42, 51–52). That is simply wrong. Even leaving aside Plaintiffs' allegations that they entrusted the government with "financial records that include bank account and credit card information," JA78 (CAC ¶146), the social security numbers indisputably stolen as

part of this hack are the very information that would enable the tax fraud, for example, that many Plaintiffs suffered. So the fact that "no plaintiff here has alleged that he provided a credit or debit card number on the SF 85 or SF 86" government forms, JA439 (Opinion 51), *still leaves the more serious incidents*. Plaintiffs are not relying just on existing payment-card fraud to establish standing.

The district court wrote that "allegations of time and sequence are all that plaintiffs provide here." JA438 (Opinion 50). What the court overlooked is the direct match between the information Defendants allowed to be compromised and the harms committed. For example, information about Plaintiff Tony Bachtell *and* his wife that was stolen in the Data Breaches was used to file fraudulent 2015 tax returns on behalf of Bachtell *and* his wife. JA40–41 (CAC ¶14). Because both Bachtells' sensitive information was taken in the Data Breaches, the fact that information about *both* Bachtells was misused in a single incident, shortly after the hack, raises an inference that the hack supplied the information used to steal their tax refund payments.

3. Plaintiffs' Harm Is Fairly Traceable to KeyPoint's Negligent Security.

The district court did not differentiate between OPM and KeyPoint in its traceability discussion, but KeyPoint will likely argue on appeal (as it did below) that it is too removed from the OPM breaches for Plaintiffs' injuries to be fairly

traceable to its negligence. That argument lacks merit given how the OPM breaches actually came about.

KeyPoint's electronic systems overlapped with OPM's, which allowed KeyPoint investigators to upload their findings directly onto the government system. JA63–64, 96 (CAC ¶¶76, 217). In spite of this linkage and the obvious target OPM's systems presented, *see* JA37, 64–65 (CAC ¶¶3, 78–80), KeyPoint failed to secure its systems in several specific ways that together constitute negligence. JA96–98 (CAC ¶¶217–23). Moreover, it was because KeyPoint allowed its security credentials to be stolen, undetected, that hackers were able to use those credentials to break into OPM's database. JA37–38, 73 (CAC ¶¶4, 6, 127). The complaint thus alleges that "KeyPoint's negligence in failing to protect and secure its user log-in credentials was a substantial factor in causing the Data Breaches." JA99 (CAC ¶228).

For these reasons, Plaintiffs' allegations meet the traceability requirement at the motion-to-dismiss stage.

C. Plaintiffs' Allegations Meet Article III's Redressability Requirement.

Although the district court did not reach the redressability element of Article III standing, it is clear that a judicial decision can redress the harm Plaintiffs suffered. Damage awards can redress their lost time and money from fraudulent tax returns, and can also compensate them for the credit monitoring and other

services they purchased after the Data Breaches: "The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages." *Attias*, 865 F.3d at 629.

* * *

All three elements of Article III standing are satisfied in this case. The district court erred by misapplying *Attias*, failing to credit Plaintiffs' factual allegations, and drawing improper inferences from selective material outside the complaint. To protect its *Attias* precedent, this Court must reverse.

II. THE DISTRICT COURT ERRED IN HOLDING THAT DERIVATIVE SOVEREIGN IMMUNITY SHIELDS KEYPOINT FROM LIABILITY.

The district court incorrectly held Plaintiffs' claims against KeyPoint barred by derivative sovereign immunity. While "government contractors obtain certain immunity in connection with work which they do pursuant to their contractual undertaking with the United States," *Brady v. Roosevelt S.S. Co.*, 317 U.S. 575, 583 (1943), that immunity applies only when the contractor's challenged conduct was "authorized and directed by the Government," *Yearsley v. W.A. Ross Constr. Co.*, 309 U.S. 18, 20 (1940), and the immunity does not apply to the contractor's "negligent exercise of that delegated power[.]" *Brady*, 317 U.S. at 583.

A. Derivative Immunity Can Apply Only When the Government Instructed the Contractor to Engage in the Challenged Conduct.

Where sovereign immunity would shield the Government from liability for certain conduct, it can also shield private entities that the Government *directs* to engage in such conduct. Thus, "derivative" sovereign immunity may apply in the "special circumstance" "[w]here the government has directed a contractor to do the very thing that is the subject of the claim[.]" *Correctional Servs. Corp. v. Malesko*, 534 U.S. 61, 74 n.6 (2001); *see Yearsley*, 309 U.S. at 21 ("[T]here is no liability on the part of the contractor for executing [the Government's] will."). Conversely, the immunity does *not* extend to "any act of [the contractor] over and beyond acts required to be performed by it under the contract[.]" *Myers v. United States*, 323 F.2d 580, 583 (9th Cir. 1963); *see also In re Fort Totten Metrorail Cases*, 895 F.Supp.2d 48, 74 (D.D.C. 2012) ("[A] key premise of *Yearsley* … is that the contractor was following the sovereign's directives.") (citations omitted).

Here, there can be no suggestion that "the government has directed [KeyPoint] to do the very thing that is the subject of the claim." *Malesko*, 534 U.S. at 74 n.6. Plaintiffs alleged that KeyPoint is liable for damages stemming from the Data Breaches because it failed to "protect and secure its user log-in credentials" and this failure "was a substantial factor in causing the" OPM breaches where "hackers accessed OPM's network using stolen KeyPoint credentials." JA73, 99 (CAC ¶¶127, 228). The Government neither "authorize[d]" nor "direct[ed]"

KeyPoint to allow derelict data security. *Yearsley*, 309 U.S. at 20. As a result, KeyPoint is not entitled to claim the Government's immunity.

The district court concluded otherwise only by adopting a broad theory of derivative immunity that transgresses the limits established by binding precedent. The district court held that, rather than protecting only conduct specifically *directed* by the Government, *Malesko*, 534 U.S. at 74 n.6, derivative immunity also protects private conduct *unless* the private conduct violates the Government's "explicit instructions[.]" JA456 (Opinion 68). This flips the settled rule on its head.

The Supreme Court specifically rejected the district court's approach in *Boyle v. United Technologies Corporation*, 487 U.S. 500, 509 (1988). *Boyle* was a products liability suit against a contractor who had manufactured certain components for a Marine helicopter. In analyzing the extent to which government contractors could claim immunity from such state tort actions, the Court discussed the "situation … in which the duty sought to be imposed on the contractor is not identical to one assumed under the contract, but is also not contrary to any assumed." *Id.* In that scenario, "[t]he contractor could comply with both its contractual obligations and the state-prescribed duty of care." *Id.* And in such a situation, *Boyle* makes clear, the contractor is *not* immune from suit. *Id.* It follows that derivative immunity can apply only where "the government has directed a

contractor to do the very thing that is the subject of the claim[.]" *Malesko*, 534 U.S. at 74 n.6 (citing *Boyle*).

The district court's contrary conclusion finds no support in its citation to *Campbell-Ewald Co. v. Gomez*, 136 S.Ct. 663 (2016). That decision holds that immunity applies to a "contractor who simply performed as the Government directed." *Id.* at 673 (quotation marks omitted). And in *Campbell-Ewald*, the Court rejected immunity where a defendant contractor had "violate[d] both federal law and the Government's explicit instructions." 136 S.Ct. at 672.

B. There Is No Derivative Immunity Where the Contractor's Challenged Conduct Breached Its Contractual Obligations to the Government.

The Privacy Act requires agencies that maintain a "system of records" containing sensitive information on individuals to "establish appropriate … safeguards to insure the security and confidentiality of [those] records and to protect against any anticipated threats or hazards to their security." 5 U.S.C. §552a (e)(10). Further, "[w]hen an agency provides by a contract for the operation by or on behalf of the agency of a system of records … the agency shall … cause the requirements of this section to be applied to such system." *Id.* §552a(m)(1). To implement this requirement, the Federal Acquisition Regulations ("FAR") mandate that when "a contract specifically provides for the design, development, or operation of a system of records on individuals on behalf of an agency … the

agency must apply the requirements of the Act to the contractor and its employees." FAR (48 C.F.R.) 24.102(c); *see also* FAR 52.224-2, 52.224-1.

Plaintiffs accordingly alleged that "[t]he contract between OPM and KeyPoint incorporates the requirements of the Privacy Act," including Section 552a(e)(10)'s requirement that KeyPoint adequately safeguard Plaintiffs' information. JA37–38 (CAC ¶123). And Plaintiffs alleged that KeyPoint *breached* this contractual duty by failing to implement several specific, industry-standard data security practices that would have prevented KeyPoint's log-in credentials from being stolen and used to extract Plaintiffs' data. JA98 (CAC ¶223). Among other deficiencies, KeyPoint failed to encrypt data, segment its network, and ensure continuous systems monitoring. *Id*. Hence KeyPoint's challenged conduct violated the Government's "explicit instructions[,]" JA455 (Opinion 67), that KeyPoint must "[c]omply with the Privacy Act" in operating its system of records. FAR 52.224-2(a)(1).

The district court reasoned that "the Privacy Act does not apply to government contractors" of its own force, and that denying immunity for KeyPoint where it breached its contractual obligation to follow the Act would "do indirectly what plaintiffs cannot do directly"—sue KeyPoint under the Act. JA457 (Opinion 69). But Plaintiffs have not asserted a Privacy Act claim against KeyPoint. Plaintiffs invoke the Act only to show that KeyPoint has breached a "duty imposed

by the Government contract," *Boyle*, 487 U.S. at 508, and is therefore not entitled to assert the *defense* of derivative immunity.

The district court also reasoned that KeyPoint was not subject to the Privacy Act on the basis that KeyPoint's systems were "deemed to be maintained by the agency" and its employees were "considered employees of the agency." JA457–58 (Opinion 69–70). However, the regulations deem the contractor's system of records "maintained by the agency" to ensure that the contractor *will* be "subject to the Act," FAR 24.102(c)—which otherwise would apply only to records "maintained by an agency[.]" 5 U.S.C. §552a (a)(4). And the contractor's employees are "considered employees of the agency" to ensure that they *will* be subject to "the criminal penalties of the Act," FAR 24.102(b)—which likewise apply of their own force only to an "officer or employee of an agency[.]" 5 U.S.C. §552a(i), (m).

The district court next held that even if the Privacy Act applied to KeyPoint by virtue of its government contract, Plaintiffs' allegations "that KeyPoint breached its contract with OPM … by 'unreasonably failing to safeguard its security credentials'" were too "conclusor[y]." JA458 (Opinion 70). To the contrary, Plaintiffs' complaint details the specific security safeguards that KeyPoint failed to establish, such as standard encryption techniques, "adequate network segmentation and layering," and "continuous system and event monitoring

and recording." JA98 (CAC ¶223). These allegations sufficiently support and render plausible Plaintiffs' allegation that KeyPoint failed to maintain adequate safeguards. JA72–73 (CAC ¶123).

The district court nevertheless wrote that Plaintiffs "can point to no provision of the contract between OPM and KeyPoint requiring [these specific security] measures." JA458 (Opinion 70). In other words, the district court thought it could disregard Plaintiffs' overarching allegation that KeyPoint failed to adequately safeguard their records as *too general*. It then reasoned that it could disregard the allegations detailing the inadequacies in KeyPoint's practices as *too specific*, since the Privacy Act merely imposes a general obligation to maintain adequate safeguards. This "heads I win, tails you lose" approach is misplaced, particularly when adjudging a motion to dismiss.

C. Derivative Immunity Does Not Protect a Contractor Who Acted Negligently.

Plaintiffs' allegations of KeyPoint's negligence provide additional grounds to reject its derivative immunity defense. That defense "is not available to contractors who act negligently in performing their obligations under the contract." *Fort Totten Metrorail Cases*, 895 F.Supp.2d at 74.

In *Brady*, the Supreme Court held that a maritime tort suit brought by the widow of a man who died from injuries sustained while boarding a vessel could proceed against the government contractor who was operating the ship. 317 U.S.

at 579. The Court acknowledged, on one hand, "that government contractors obtain certain immunity in connection with work which they do pursuant to their contractual undertaking with the United States," *id.* at 583—but that principle did not mean that such contractors "can escape liability for a *negligent* exercise of that delegated power[.]" *Id.* (emphasis added); *see also Ackerson v. Bean Dredging LLC*, 589 F.3d 196, 207 (5th Cir. 2009); *Fort Totten*, 895 F.Supp.2d at 74–75.

Here, as in *Brady*, Plaintiffs seek to hold KeyPoint liable for its "own negligence[.]" 317 U.S. at 580. Plaintiffs have plausibly alleged that: (1) KeyPoint "owed a duty of care to Plaintiffs" because it was entrusted with their sensitive information, JA96–97 (CAC ¶¶218–21), (2) KeyPoint breached that duty by unreasonably failing to take numerous specific security measures that are recognized and standard in the industry, JA98 (CAC ¶223), and (3) this breach of duty caused Plaintiffs harm. JA81–83, 99 (CAC ¶¶163, 228).

The district court, however, questioned whether even negligent conduct forecloses derivative immunity. The court attempted to distinguish *Brady*, stating that the Supreme Court there "assume[d] that by contract [the defendant] will be exonerated or indemnified [by the federal government]," and "KeyPoint will not be indemnified by the federal government in this case[.]" JA460 (Opinion 72 n.33 (third alteration in original)). But this distinction is unavailing because the indemnity provision stood apart from the derivative immunity argument in *Brady*.

That is, in *addition* to claiming the government's immunity derivatively, the contractor *also* claimed the suit could not go forward under a federal statute foreclosing maritime torts against the United States, because the indemnity provision in its government contract made the United States "the real party in interest." 317 U.S. at 582.

Finally, the district court stated that even if negligence forecloses derivative immunity, there are "only conclusory allegations that KeyPoint … acted negligently." JA460 (Opinion 72). But in fact, the complaint specifies several data security measures that—despite being standard in the industry—KeyPoint failed to implement. JA98 (CAC ¶223).

III. THE DISTRICT COURT ERRED IN HOLDING THAT PLAINTIFFS' COMPLAINT DOES NOT STATE A CLAIM UNDER THE PRIVACY ACT.

If an agency fails to comply with the safeguards provision, 5 U.S.C. §552a (e)(10), "in a manner which was intentional or willful," and "in such a way as to have an adverse effect on an individual," he or she may recover "actual damages sustained" in an amount no less than $1,000. *Id.* §§552a(g)(1)(D), (g)(4). The district court recognized that Plaintiffs plausibly alleged that OPM intentionally chose not to establish the safeguards necessary to protect their records, *see* JA444–45 (Opinion 56–57), and that at least two Plaintiffs plausibly alleged "actual damages." The court deemed it implausible, however, that those damages were

proximately caused by OPM's willful violations of the Act. But the CAC adequately alleges that more than two Plaintiffs suffered actual damages, and that these damages were caused by OPM's ineffective safeguards.

The Privacy Act claim should be reinstated.

A. Plaintiffs Have Adequately Alleged Actual Damages.

The Supreme Court has held that the "actual damages" required by the Privacy Act are equivalent to "special damages" at common law: "actual—that is, pecuniary or material—harm." *FAA v. Cooper*, 566 U.S. 284, 296 (2012). The CAC sufficiently alleges pecuniary harm to Plaintiffs.

First, because Jane Doe's and Charlene Oliver's "[d]irect out-of-pocket expenses … are the very definition of pecuniary losses," *Hill v. DOD*, 70 F.Supp.3d 17, 21 (D.D.C. 2014), the district court correctly concluded that these Plaintiffs suffered "'actual damages' under the [Privacy] Act." JA443 (Opinion 55).

Second, several other Plaintiffs sustained actual damages from unauthorized account openings in their names, unauthorized charges, or other financial fraud.[8] The district court held otherwise by presuming these fraudulent charges had been

[8] For instance, Kelly Flynn and her husband had two credit cards fraudulently opened in her name, two other credit cards opened in her husband's name, and fraudulent loans totaling $6,400 taken out in each of their names. JA48–49 (CAC ¶28).

reimbursed. JA423, 442 (Opinion 35, 54). But the "well entrenched" rule for determining whether a plaintiff experienced actual damages is that "an injured person may usually recover in full from a wrongdoer regardless of anything he may get from a 'collateral source' unconnected with the wrongdoer." *Kassman v. American Univ.*, 546 F.2d 1029, 1034 (D.C. Cir. 1976).

Third, many Plaintiffs spent significant amounts of time working to resolve the misuse of their personal information. Lillian Gonzalez-Colon had "to take time off work" to attempt to resolve a fraudulent tax filing and close a fraudulent Verizon account. JA50–51 (CAC ¶31). These lost hours, which Plaintiffs could have spent engaging in gainful activity, constitute pecuniary harm under the Privacy Act. *See Beaven v. DOJ*, 622 F.3d 540, 558–59 (6th Cir. 2010); *Makowski v. United States*, 27 F.Supp.3d 901, 914 (N.D. Ill. 2014) ("Loss of economic opportunity is pecuniary harm.").

Fourth, several Plaintiffs experienced tax fraud that either delayed receipt of their tax refunds, cost many hours of lost time to resolve, or both. The IRS informed Kelly Flynn after the Data Breaches, for example, that "a fraudulent tax return for the 2014 tax year had been filed using her and her husband's personal information." JA48–49 (CAC ¶28). As of March 2016 she was still waiting to receive her federal and state tax refunds for 2014. *Id.*

Fifth, many Plaintiffs incurred hard costs or spent valuable time mitigating damage from the Data Breaches, including by purchasing credit monitoring services or credit reports to scrutinize for fraudulent activity. Such "fees associated with running a credit report" are "pecuniary expenses" that constitute "actual damages" under the Privacy Act. *Doe v. Chao*, 540 U.S. 614, 626 n.10 (2004); *see also VA Data Theft*, 2007 WL 7621261, at *4 n.7.

B. The District Court Erred by Rejecting Plaintiffs' Allegations That Their Damages Were Proximately Caused by OPM's Willful Failure to Protect Their Data from Known Risks.

Lastly, the district court erred when it rejected Plaintiffs' allegations that their injuries were "'a result of' the OPM's actions[.]" JA446 (Opinion 58). At the pleading stage, a Privacy Act plaintiff "must only plausibly allege proximate causation." *Hill*, 70 F.Supp.3d at 22.

It is absolutely plausible that identity fraud, such as false tax returns and the opening of unauthorized accounts in Plaintiffs' names, resulted from the theft of their social security numbers, birthdates, and addresses in the Data Breaches. *See SAIC*, 45 F.Supp.3d at 31; *Welborn v. IRS*, 218 F.Supp.3d 64, 79 (D.D.C. 2016) (finding a plausible "causal connection" between social security number theft and fraudulent tax return). The timing of Plaintiffs' injuries—in the months immediately following the Data Breaches—further reinforces the causal link between the two. *See Makowski*, 27 F.Supp.3d at 914 (causation plausible where

"[t]he complaint alleges an unbroken chain of events" from Privacy Act violation to injury). And the various mitigation costs that Plaintiffs incurred are the immediate result of OPM's security failures. Consequently, the district court erred when it rejected Plaintiffs' allegation that their damages are "directly traceable to OPM's violations [of the Privacy Act]." JA89 (CAC ¶185).

CONCLUSION

For the foregoing reasons, the judgment should be reversed.

Respectfully submitted,

Dated: May 15, 2018

/s/ *Jordan Elias*

Daniel C. Girard
Jordan Elias
GIRARD GIBBS LLP
601 California St., 14th Floor
San Francisco, CA 94108

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Ave., N.W.
Washington, D.C. 20036

John Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin St., 7th Floor
Tampa, FL 33602

Tina Wolfson
AHDOOT & WOLFSON, PC
10728 Lindbrook Dr.
Los Angeles, CA 90024

Plaintiffs' Steering Committee

Gary E. Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Ave., N.W.
Suite 305
Washington, D.C. 20016

Liaison Counsel

Norman E. Siegel
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112

Plaintiffs' Counsel

Richard B. Rosenthal
THE LAW OFFICES OF RICHARD B. ROSENTHAL
1581 Brickell Ave.
Suite 1408
Miami, FL 33129

Appellate Counsel

CERTIFICATE OF COMPLIANCE

This brief complies with the Court's March 26, 2018 Order regarding word limitations, because it contains 11,993 words, as determined by Microsoft Word, including the headings and footnotes and excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), which, when added to the words in the NTEU Plaintiffs' opening brief, do not exceed the allotted 22,000 words. The brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6). The text appears in 14-point Times New Roman, a proportionally spaced serif typeface.

Dated: May 15, 2018 /s/ *Jordan Elias*

Counsel for Class Plaintiffs–Appellants

CERTIFICATE OF SERVICE

I hereby certify that on May 15, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit, via the appellate CM/ECF system. Case participants who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: May 15, 2018

/s/ *Jordan Elias*

Counsel for Class Plaintiffs–Appellants