RECORD NO. 15-1395(L)
CONSOLIDATED W/15-1715

IN THE
United States Court of Appeals
FOR THE FOURTH CIRCUIT

RECORD NO. 15-1395

RICHARD G. BECK; LAKRESHIA R. JEFFERY; BEVERLY WATSON; CHERYL GAJADHAR; JEFFERY WILLHITE, on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

v.

ERIC K. SHINSEKI, in his official capacity as Secretary of Veterans Affairs; TIMOTHY B. MCMURRY, in his official capacity as the former Medical Director of William Jennings Bryan Dorn VA Medical Center; BERNARD L. DEKONING, in his official capacity as the Chief of Staff of William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD, RN, Director for Patient Care-Nursing Services of William Jennings Bryan Dorn VA Medical Center; JON ZIVONY, Assistant Director of William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA, in his official capacity as the Associate Director of William Jennings Bryan Dorn VA Medical Center,

Defendants-Appellees.

RECORD NO. 15-1715

BEVERLY WATSON, on behalf of herself and all others similarly situated

Plaintiff-Appellant,

v.

ROBERT A. MCDONALD, in his official capacity as Secretary of Veterans Affairs;TIMOTHY B. MCMURRY, in her official capacity as the Medical Directorof William Jennings Bryan Dorn VA Medical Center; RUTH MUSTARD,RN, in her official capacity as the Associate Director for Patient Care/Nursing Servicesof William Jennings Bryan Dorn VA Medical Center; DAVID L. OMURA,in his official capacity as the Associate Director of William Jennings Bryan Dorn VAMedical Center; JON ZIVONY, in his official capacity as Assistant Director of William Jennings Bryan Dorn VA Medical Center; SUE PANFIL, in her official capacity as the Privacy Officer of William Jennings Bryan Dorn VA Medical Center,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA AT COLUMBIA

OPENING BRIEF OF APPELLANTS

COUNSEL LISTED ON BACK OF COVER

LANTAGNE LEGAL PRINTING 801 East Main Street Suite 100 Richmond, Virginia 23219 (804) 644-0477
A Division of Lantagne Duplicating Services

RECORD NO. 15-1395(L)
CONSOLIDATED W/15-1715

D. Michael Kelly
Bradley D. Hewett
Mike Kelly Law Group, LLC
500 Taylor Street
Post Office Box 8113
Columbia, South Carolina 29202
(803) 726-0123
mkelly@mklawgroup.com
bhewett@mklawgroup.com

Douglas J. Rosinski
Douglas J. Rosinski, Esq., Inc.
Suite 150-450
701 Gervais Street
Columbia, SC 29201-3066
(803) 256-9555
djr@djrosinski.com

Counsel for Appellants

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fourth Circuit Local Rule 26.1, Appellants make the following disclosures:

1. Is said party a publicly held corporation or other publicly held entity?

   Answer: No.

2. Does said party have any parent corporations?

   Answer: No.

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity?

   Answer: No.

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(b))?

   Answer: No.

5. Is party a trade association?

   Answer: No.

/S/ BRAD D. HEWETT

Dated: August 10, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS

OTHER

JURISDICTIONAL STATEMENT

The federal courts have subject matter jurisdiction because this civil matter raises questions of federal law under the Administrative Procedure Act, 5 U.S.C. §§ 701-706 and the Privacy Act of 1974, 5 U.S.C. § 552(a) (the "Privacy Act"). 28 U.S.C. § 1331.

This Court has jurisdiction because these appeals are from final orders of the United States District Court for the District of South Carolina entered on March 31, 2015 ("*Beck* Order"), and June 15, 2015 ("*Watson* Order"). 28 U.S.C. §§ 1291, 1294. These appeals are timely because Appellants filed a Notice of Appeal in *Beck v. McDonald*, No. 15-1395 *("Beck")* on April 14, 2015, and for *Watson v. McDonald*, No. 15-1715 *("Watson")* on June 29, 2015, which are within the period allowed by law. 28 U.S.C. § 2107(b).

STATEMENT OF ISSUES

I. An "adverse effect" on an individual from an agency action provides Article III standing under the Privacy Act and the Administrative Procedure Act. *Clapper v. Amnesty Int'l USA* did not require a higher standard of injury-in-fact on the record in this case. The District Court erred in applying the wrong standard to conclude that Appellants lacked Article III standing.

II. The record established that Dorn has never been in full compliance with the Privacy Act. The District Court concluded that VA's past conduct was insufficient to show that a present case or controversy exists. The District Court erred because on this record there was no factual basis for its conclusion that VA would comply with the Privacy Act in the future.

III. The Administrative Procedure Act authorizes the courts to compel agency action unlawfully withheld or unreasonably delayed. The District Court concluded that an action to require compliance with specific procedural steps which the agency previously determined were required to safeguard personal information was improperly seeking "compliance with broad statutory mandates." The District Court erred in failing to compel the agency to comply with its own specific procedural requirements.

STATEMENT OF CASE

Statement of Facts

Beck v. McDonald, No. 15-1395

Appellants are honorably discharged veterans who have received health care at the William Jennings Dorn VA Medical Center ("Dorn") in Columbia, South Carolina. On February 11, 2013, a laptop computer was stolen from the Dorn pulmonology laboratory. JA2, 824. The laptop computer contained the private

personal and medical information of patients who had received or were receiving medical treatment at Dorn. Officials were unsure of the exact number of individuals affected or the precise personal information on the laptop, but estimated approximately 7,500 from reviewing examination schedules and interviewing the device operator. JA583, 588-590. The personal information on the laptop computer was not encrypted nor were the Privacy Act physical, administrative, or technical safeguards implemented as required by law, policy, accepted industry standards, and repeated public representations by the Department of Veterans Affairs ("VA" or "Department"). *See, e.g.*, JA2, 5-6, 8-9, 823-824.

As a result, the Medical Director at Dorn formally appointed an Administrative Investigation Board ("AIB") to investigate the incident. JA778. The AIB concluded that policies and procedures for using the laptop were not followed, there was a failure to ensure compliance with VA policies, and that there was clear negligence on the part of Dorn related to the encryption of the laptop. JA823-824. Dorn subsequently notified the individuals it believed were affected of the data breach and the Secretary's determination that they were legible for one year of credit monitoring. JA25-28, 195-197.

Few if any VA officials appeared surprised by the incident. Shortly after the laptop theft, a VA official stated in an email that "[t]hese occurrences are going to

happen. It goes on throughout the VA." JA44. A VA "Information Security Officer" emailed that there had been "an original data call back in December of 2011 that most Biomed folks ignored (see attached) (DON'T QUOTE ME ON THAT!), that probably precipitated this incident." JA43. A Dorn official emailed that "this does not surprise me and this is why biomedical devices will continue to be vulnerable because VA will not hold the vendors feet to the fire and make them play by our rules …. [S]ince we don't know how or whom, the same thing can happen again." JA43. Within the same email exchange, Dorn's Facility Information Security Officer conceded that officials did not even know how many devices similar to the stolen laptop were in the facility. JA40 (observing that "We cannot protect what we cannot identify or do not know is out there.").

Dorn's then-Privacy Officer, later testified that Dorn personnel did not secure patient information, completely disregarded patient privacy, failed to take any initiative to protect veterans' personal information, and that the relevant records management policy and information security policy were not followed. JA814-815, 817-818. Her testimony was validated by the results of the AIB investigation. Dorn's Chief of Respiratory Therapy stated that "[t]he laptop was not secured or encrypted nor was the log-on for access to the software." JA795. The operator of the stolen laptop was completely unaware that the laptop was unencrypted and

admitted that the laptop should have been more protected. JA791. The Dorn Chief of Biomedical Engineering, testified that he did not know whether any attempt to encrypt the laptop had ever been made. JA800. Dorn also failed to require a password to access the laptop computer. JA788-789. The pulmonary technician that used the stolen laptop testified that he would turn on the laptop in the morning and work on it all day without entering a password. JA789.

The VA Director of Field Security testified that Dorn did not comply with VA requirements to encrypt the laptop. JA742, 743-744. This official confirmed that the stolen laptop was not password protected and that Dorn had failed to inventory the laptop as required by VA policy. JA771-73, 777. He also testified that Dorn did not comply with requirements to maintain control of keys to offices containing laptops storing personal identifying information. JA747-748. He also testified and confirmed that the laptop was not cable locked, was not stored in a locked computer cabinet, and was not installed with an anti-theft device – all violations of VA policy and, therefore, Dorn was not in compliance with VA requirements. JA768-769, 771-773.

The former Privacy Officer at Dorn testified that an individual did not even need a badge or any office credentials to access the Dorn area where the laptop was stolen. J582. The AIB investigation showed that, contrary to VA procedures,

Dorn had also not re-cored the locks in the area where the laptop was stored for at least three years, JA828, although discovery established that at least five *former* employees may still have a key to the room from which the laptop was stolen. JA279. A key may not have been needed to steal the laptop, however, as the AIB found routine staff failures to lock the room, JA797, 807, despite recent thefts in the same area – although the area was supposedly secure. JA793.

Dorn procedures required that "Staff *shall lock* down" laptop computers when not in use. JA837. The VA Region 3 Division Chief confirmed that "the laptop also *should have been cabled* to whatever it had." JA784 (emphasis added). Yet, the stolen laptop "was *only attached via a Velcro strip, no cabling* and had no identifiable bar code identification." JA198 (emphasis added); *see also* JA794 ("The only thing that connected it was a piece of double stick Velcro").

The Veterans Health Administration Privacy Compliance Assurance Officer testified that Dorn has never been fully compliant with VA privacy procedures. JA140-141. He also testified that VA could not determine whether Dorn had installed reasonable physical safeguards. JA141-145. He further testified that VA management agreed with the AIB report regarding Dorn's failures to physically safeguard the laptop and did not dispute the facts and conclusions contained in the AIB final report. JA146, 147-148.

On the date that the laptop was stolen, VA had numerous mandatory administrative procedures in place to ensure that the required technical and physical safeguards were adequately implemented. The controlling Dorn requirements were largely detailed in the "Reasonable Privacy and Security Safeguards" section of Medical Center Memorandum 544-1023 "Privacy Policy." JA825. This document explicitly stated that: "*All members of the workforce are responsible* for complying with this privacy policy, applicable federal laws and regulations, the Department of Veterans Affairs (VA) regulations and policies, Veterans Health Administration (VHA) policies, as well as the procedures and practices developed in support of these policies." JA831 (emphasis added); *see also* JA825 ("All facility workforce members shall ensure that appropriate administrative, technical, and physical safeguards are used"). Further, Dorn "Executive Management (Medical Center Director, Associate Director, Chief Nursing Executive, Chief of Staff) is responsible for," among other things, "to support the Privacy Program and *ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy* and other federal legislation (e.g., . . . Privacy Rule (45 C.F.R. Parts 160 and 164), the Privacy Act . . .). JA832.

VA requirements also existed to identify, track, and physically inventory equipment as specified in VA Handbook 7002, Part 13, "Control and Inventory of

IT Equipment." JA841. Further, as a result of a December 30, 2011, memorandum, "all biomedical shops in the VISN know that they need to identify" devices such as the stolen laptop. JA821. Yet, when asked about the number of "biomedical laptops" in the facility similar to the missing device, the Dorn Information Security Officer could not provide an exact number. JA822 ("It's one of the things we're trying to get full wraps around"). In response to a statement by an investigator who found it "hard to believe or kind of surprising that a piece of equipment could possibly have been brought into the facility *skipping the whole receiving process* possibly by a vendor straight to a service line," the Dorn Chief of Logistics, unequivocally stated: "Unfortunately *I know for a fact that happens*." JA785-786 (emphasis added). VA's Region 3 Division Chief stated that "my understanding is the [stolen] laptop . . . didn't come in through property management, didn't even have a tag on it." JA782.

Dorn was also required to provide the necessary resources to support the VA's Privacy program. JA832 (provide "the necessary resources (funding and personnel) to support the Privacy Program")). The then-Privacy Officer testified that she did not have sufficient staff and multiple requests for additional staff had been denied. JA71-76, 125, 132. She further testified that as the sole privacy officer, she was responsible for training 2,000 employees on privacy requirements.

JA71-72. She also testified that her internal audits had never revealed that there were unencrypted laptops at Dorn. JA83.

Watson v. McDonald, No. 15-1715

Dorn announced on September 8, 2014, while *Beck* was still being litigated, that four boxes of pathology reports went missing from the facility on July 14, 2014. These boxes of records contained the names, *full* Social Security numbers, and confidential medical and disability information of at least 2,179 veterans. JA51. Beverly Watson received a letter from Dorn advising that her personal information was contained in one of the boxes of missing records. JA195-197. Ms. Watson is a named plaintiff in the *Beck* litigation and also received a letter from Dorn a result of that February 2013 data breach.

In her Complaint, Ms. Watson alleged that at the time of these two incidents, Appellees were required, at a minimum, to comply with the "Privacy Act Guidelines – July 1, 1975" published in the Federal Register on July 9, 1975, unless the requirements therein were subsequently modified or eliminated. JA55. In addition, Appellees were required to comply with numerous federal statutes, regulations, technical standards, as well as VA policies, procedures, and rules promulgated since the VA's 2006 loss of a laptop containing the personal information of 26 million veterans. JA55. Ms. Watson also alleged that VA

regulations and numerous VA policies, directives, and procedures required Appellees to safeguard individuals against an invasion of privacy, to collect, maintain, use, or disseminate records of personally identifiable information in a manner that assured that such action was for a necessary and lawful purpose, and to ensure that adequate safeguards are provided to prevent misuse of such information. JA55.

Procedural History

Beck v. McDonald, No. 15-1395

On April 12, 2013, Richard G. Beck and Lakreshia R. Jeffery filed a class action lawsuit against the Secretary of Veterans Affairs and other officials at Dorn, alleging violations of the APA, Privacy Act, and negligence claims. On July 1, 2013, Appellants filed an Amended Complaint to include Beverly Watson, Cheryl Gajadhar, and Jeffery Willhite as named plaintiffs ("Plaintiffs"). On July 16, 2013, VA filed a motion to dismiss the Amended Complaint on the basis that Plaintiffs failed to state a claim and the court lacked subject matter jurisdiction because Appellants did not have Article III standing.

On November 19, 2013, the district court entered an Order granting VA's motion to dismiss Plaintiffs' negligence claims, while denying the Motion to Dismiss as to Plaintiffs' claims for violations of the APA and Privacy Act. After

preliminary discovery, Plaintiffs filed a Motion for Summary Judgment on June 30, 2014, and subsequently a Motion for Class Certification on July 21, 2014. After several months of additional discovery, including expert identifications and numerous depositions of named parties and VA officials, VA filed a Motion to Dismiss and, in the alternative, Motion for Summary Judgment on December 16, 2014. On January 28, 2015, the district court conducted a hearing on the Plaintiffs' Motion for Summary Judgment, Plaintiff's Motion to Certify Class, and VA's Motion to Dismiss, and, in the alternative, for Summary Judgment.

On March 31, 2015, the district court entered an Order granting VA's Motion to Dismiss and, in the alternative, Motion for Summary Judgment, holding that Plaintiffs lacked Article III standing to bring claims under the APA and Privacy Act. In its Order, the district court dismissed as moot Plaintiffs' Motion for Class Certification and denied Plaintiffs' Motion for Summary Judgment. On April 14, 2015, Plaintiffs filed a Notice of Appeal of the District Court's March 31, 2015, final order. On April 16, 2015, this case was opened on appeal for the Fourth Circuit. No. 15-1395, Dkt. No. 1.

Watson v. McDonald No. 15-1715

On September 9, 2014, Beverly Watson filed a class action lawsuit against the Secretary of Veterans Affairs and other officials at Dorn, alleging violations of the

APA and the Privacy Act. On November 12, 2014, VA filed a Motion to Dismiss on the basis that Watson failed to state a claim and the court lacked subject matter jurisdiction because Appellants did not have Article III standing.

On June 15, 2015, the district court entered an Order granting VA's Motion to Dismiss for lack of subject matter jurisdiction. On June 29, 2015, Ms. Watson filed a Notice of Appeal of the District Court's March 31, 2015, final order. On June 30 , 2015, this case was opened on appeal for the Fourth Circuit. No. 15-1715, Dkt. No. 1.

On July 8, 2015, this Court granted Appellants' motion to consolidate the *Beck* and *Watson* cases, with *Beck* as the lead case. *See* No. 15-1395 (L), Dkt. No. 32.

SUMMARY OF ARGUMENT

The District Court erred in concluding that Appellants did not have Article III standing to pursue their Privacy Act and Administrative Procedure Act claims. The District Court improperly applied a heightened standard by reading too much into *Clapper v. Amnesty Int'l USA* and failing to factually distinguish *City of Los Angeles v. Lyons*. As a result, the District Court erroneously required a showing of much more than required by controlling law to establish standing under either Act.

Applying the properly legal standards for standing in cases where a data breach has already occurred, Appellants have established that they have suffered "adverse effects" sufficient to open the courthouse door to their Privacy Act claims. Similarly, Appellees have established standing to pursue their Administrative Procedure Act claims as individuals "adversely affected" by VA's failure to adequately implement Privacy Act safeguard requirements. Further, contrary to the District Court, it does have authority under the Administrative Procedure Act to provide Appellants with the equitable relief they seek because of VA's history of recalcitrance in admittedly failing to have *ever* established compliance with Privacy Act requirements.

ARGUMENT

This Court reviews *de novo* a district court dismissal for lack of subject matter jurisdiction. *Taylor v. Kellogg Brown & Root Servs. Inc.*, 658 F.3d 402, 408 (4th Cir. 2011). The burden of establishing standing falls on the party claiming subject matter jurisdiction. *Frank Krasender Enters. v. Montgomery Cnty.*, 401 F.3d 230, 234 (4th Cir. 2005). In reviewing the dismissal of a complaint, the Court must "assume all well-pled facts to be true" and "draw all reasonable inferences in favor of the plaintiff." *Nemet Chevrolet Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 253 (4th Cir. 2009) (internal quotation marks and alterations omitted). In doing so, the court must consider "documents incorporated into the complaint by reference." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

A court may dismiss a complaint under Federal Rule of Civil Procedure 12 *only* if it is clear that no relief could be granted under any set of facts that could be proved consistent with the allegations. *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999). "[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and 'that a recovery is very remote and unlikely.'" *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)).

This Court reviews *de novo* the district court's granting of summary judgment. *Laber v. Harvey*, 438 F.3d 404, 409 (4th Cir. 2006). Summary judgment is only appropriate where the record taken as a whole would not allow a rational trier of fact to find for the nonmovant. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). The party moving for summary judgment "has the burden of establishing that there is no issue as to any material fact." *Cooper v. United States*, 903 F.Supp. 953, 955 (D.S.C. 1995). In considering a summary judgment motion, "the inferences to be drawn from the underlying facts must be viewed in the light most favorable to the non-moving party. *Matsushita Electric Industrial Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

It is well established summary judgment should be granted "only when it is clear that there is no dispute concerning either the facts of the controversy or the inferences to be drawn from those facts." *Pulliam Inv. Co. v. Cameo Properties*, 810 F.2d 1282, 1286 (4th Cir. 1987). Summary judgment is proper only when, viewing the facts in the light most favorable to the non-moving party, the moving party is entitled to judgment as a matter of law. *Blair v. Defender Servs.*, 386 F.3d 623, 625 (4th Cir. 2004). To demonstrate entitlement to judgment as a matter of law, the party moving for summary judgment must first present evidence demonstrating the absence of a genuine issue of material fact. *Temkin v. Frederick*

County Comm'rs, 945 F.2d 716, 718 (4th Cir. 1991); *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). The non-moving party "is entitled to the presumption that all his evidence is credible," *Miller v. Leathers*, 913 F.2d 1085, 1087 (4th Cir. 1990), and "to the most favorable inferences that may reasonably be drawn from the forecasted evidence." *Ross v. Communications Satellite Corp.*, 759 F.2d 355, 364 (4th Cir. 1985).

I. Article III Standing Exists Under The Controlling Law For Both Privacy Act and APA Claims

The District Court erred in concluding that Appellants lacked Article III standing to pursue their Privacy Act and Administrative Procedure Act claims because it did not apply the proper legal standards.

A. The District Court Misapplied Controlling Law

Plaintiffs have standing to proceed to trial and obtain relief. "The standing inquiry ensures that a plaintiff has a sufficient personal stake in a dispute to render judicial resolution appropriate." *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 153 (4th Cir. 2000) (en banc) (*Gaston Copper I"*). In *Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, the United States Supreme Court provided, in part:

> At an irreducible minimum, Art. III requires the party who invokes the court's authority to show [1] that he personally has suffered some actual *or threatened* injury as a result of the putatively illegal conduct

> of the defendant ... and [2] that the injury fairly can be traced to the challenged action and [3] is likely to be redressed by a favorable decision.

454 U.S. 464, 472 (1982) (internal quotation marks and citations omitted) (emphasis supplied); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). These three prongs are most commonly referred to as (1) injury-in-fact, (2) traceability, and (3) redressability. *American Canoe Ass'n v. Murphy Farms, Inc.*, 326 F.3d 505, 517 (4th Cir. 2003). Only "injury-in-fact" is at issue here. JA 1046, 1080.

This Court has held that an enhanced risk of harm may constitute injury-in-fact. *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 629 F.3d 387, 394 (4th Cir. 2011) (en banc) (*Gaston Copper II*) (plaintiff "established an injury in fact by asserting a reasonable fear and concern about the effects of" defendant's action); *see also 1000 Friends of Maryland v. Browner*, 265 F.3d 216, 225-26 (4th Cir. 2001) (threat of future exposure to pollutants found "a sufficiently concrete, imminent injury" to confer standing); *Gaston Copper I* at 153 ("Threats or increased risk constitutes cognizable harm" sufficient to satisfy the injury-in-fact requirement). As discussed further below, Appellants alleged and the record established that there is and will remain a threatened risk of identity theft and associated harms because of Defendants' actions and inactions. In addition, the

government itself has determined such risks of harm are real. *See, e.g.*, JA739; *see also Perkins v. VA*, No. 2:07-cv-00310-IPJ, Dkt. No. 72, at 5-6 (N.D. Ala. Apr. 10, 2010) (quoting March 28, 2007, letter from the Centers for Medicaid and Human Services to VA Assistant Secretary for Office of Information and Technology) ("there is *a high risk* that the loss of personally identifiable information may result in *harm to the individuals* concerned." (emphasis supplied)); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007) (citing a Government Accountability Office report that finds that "stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.").

Other jurisdictions have explicitly extended the *Gaston Copper* analysis to data breaches. In *Krottner v. Starbucks Corp.*, the Court of Appeals for the Ninth Circuit applied *Gaston Copper II* and *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007), in analyzing whether employees' allegation that the theft of a company laptop subjected them to increased risk of future identity theft was sufficient to establish injury-in-fact for Article III standing. 628 F.3d 1139 (9th Cir. 2010). As here, *Krottner* involved a stolen laptop, in that case containing the unencrypted names, addresses, and social security numbers of approximately

97,000 Starbucks employees. Much like the letter received by the 7,405 veterans whose personal information was on the stolen Dorn laptop, Starbucks sent a letter to the affected employees stating that it had "no indication that the private information had been misused," but offered credit watch services for the employees for the next year. *Krottner,* 628 F.3d at 1141.

The *Krottner* Court, citing to *Gaston Copper II,* held that the employees had sufficient standing to proceed as they had alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data. *Krottner,* 628 F.3d at 1143. The court further reasoned that the employees' claims might be conjectural or hypothetical (as the District Court concluded below) *if no laptop had been stolen* and the employees had *sued based on the risk that it would be stolen* at some point in the future. *Id.* The same logic applies in *Beck* and *Watson* because the laptop was stolen and the suits are based on the risk arising from an already occurring event. JA2, 51.

A broad cross-section of courts, including the Second, Sixth, Seventh, and Ninth Circuit Courts of Appeal, now have granted standing on the basis that the risk of future harm is injury-in-fact. Of particular note, the Court of Appeals for the Seventh Circuit recently found sufficient injury-in-fact from the increased risk of identity theft to convey Article III standing *after* applying *Clapper v. Amnesty*

Int'l USA, 133 S. Ct. 1138 (2013). *Remijas v. Neiman Marcus Group, LLC*, 2015 U.S. App. LEXIS 12487 (7th Cir. Jul. 20. 2015). *Remijas* continues and extends the pre-*Clapper* line of decisions similarly finding standing in such cases. *See, e.g., Pisciotta v. Old National Bancorp.*, 499 F.3d 629, 634 & n.3 (7th Cir. 2007); *Denney v. Deutsche Bank AG*, 443 F.3d 253 (2nd Cir. 2006); *Sutton v. St. Jude Medical S.C., Inc.*, 419 F.3d 568, 572 (6th Cir. 2005); *Central Delta Water Agency v. U.S.*, 306 F.3d 938, 948 (9th Cir. 2002). There is plainly nothing novel about standing based on the risk of future harm in data breach cases, indeed the trend is moving towards that result. Appellants respectfully request that this Court explicitly adopt this standard.

B. Appellants Have Standing For Their Privacy Act Claims Under Chao's "Adverse Effect" Standard

The District Court also erred by requiring more than an "adverse effect" from Defendants' Privacy Act violations to establish Article III standing. "Whenever any agency . . . fails to comply with any other provision of [5 U.S.C. § 552a], or any rule promulgated thereunder, in such a way as to have an *adverse effect* on an individual . . . the individual may bring a civil action against the agency." 5 U.S.C. § 552a(g)(1)(D) (emphasis supplied).

> [T]he reference in [5 U.S.C.] § 552a(g)(1)(D) to "adverse effect" acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and

> *who may consequently bring a civil action without suffering dismissal for want of standing to sue*.

Doe v. Chao, 540 U.S. 614, 624 (2004) (emphasis supplied); *see also* JA971-973, 996-997. Removing any doubt about the meaning of this statement, the Supreme Court further stated "[t]hat is, an individual subjected to an adverse effect has injury enough to open the courthouse door," although "more" is required for a "cause of action for damages under the Privacy Act." *Id*. at 624-25.

Contrary to *Chao*, however, the District Court required Appellants to demonstrate much "more" to maintain their action below. *See, e.g.*, JA1057 ("failed to show that the risk of identity theft is 'certainly impending'"); JA1058 ("failed to show that [] increased risk suffices to confer standing"); JA1059 ("record shows no intent or attempt to misuse any Plaintiff's personal information"); 1060 ("fail to meet the 'substantial risk' standard"); 1091 ("Plaintiff has not alleged – or asserted facts to make a plausible an allegation – that the identity theft she fears is 'certainly impending'"); JA1092 ("Although Plaintiff need not show that it is literally certain that her identity will be stolen, she has failed to allege facts that would plausibly establish an 'imminent' or 'certainly impending' risk that she will be victimized."). These are not the tests to "open the courthouse door" under *Chao*. The District Court erred, therefore, by requiring such showings to establish Article III standing.

The District Court's error was prejudicial because Appellants did assert sufficient "adverse effects" to open the courthouse door. Ms. Gajadhar repeatedly checks her credit reports and monitors her financial account activity because someone has tried to make several unauthorized purchases using her account. *See* JA336-338 **(**notified by Wells Fargo of an unauthorized $700.50 purchase and multiple unauthorized attempts to purchase insurance for $199.00). Jeffery Willhite desires to obtain credit monitoring but cannot afford the service. JA972. Some of the Appellants have experienced emotional upset, fear identity theft and financial fraud, and feel obligated to check their accounts each day as well as to continue paying for credit monitoring. JA3, 12, 485, 488-489, 999-1000. These are all adverse effects, which under *Chao* "satisfy[y] the injury-in-fact and causation requirements of Article III standing." 540 U.S. at 624. The District Court's failure to address this issue was prejudicial legal error.

C. Clapper Cannot Bear The Weigh Placed On It By The District Court

The District Court erred in concluding that *Clapper* changed the standards for Article III standing. *See, e.g.*, JA1057 ("A reasonable concern of future harm may satisfy the less onerous standing requirements at play in environmental cases, but *Clapper* requires more."); *see also* JA1090-1091. Injury-in-fact from the increased risk of identity theft exists after *Clapper*. *Remijas*, 2015 U.S. App. LEXIS 12487.

It is "important not to overread *Clapper*." *Id.* at *14; *see also In re Adobe Sys. Privacy Litig.*, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal 2014) ("*Adobe*") at *24 ("*Clapper* did not change the law governing Article III standing."). Contrary to the District Court, therefore, *Clapper* did not establish a new test for Article III standing.

A "reasonable concern" is the standard for Article III standing in this jurisdiction. *Friends of the Earth, Inc. v. Laidlaw Environmental Servs*, 528 U.S. 167, 183-85 (2000); *Gaston Copper* II at 397. Yet, the District Court read *Clapper* to mean that "the environmental cases holding that 'reasonable concerns' of harm suffice to confer standing do not control the standing inquiry currently before this Court." JA1057, 1091. Contrary to the District Court's implied conclusion, therefore, *Clapper* did not overrule this controlling case law.

The Seventh Circuit unequivocally distinguished *Clapper* from cases where the data theft had already occurred and found Article III standing existed based on future injuries arising from that event. *Remijas,* 2015 U.S. App. LEXIS 12487 at *11 ("*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing."). The *Remijas* Court noted that the Supreme Court decided that the *Clapper* plaintiffs "did not have standing" because "they could not show that their communications with suspected terrorists *were* intercepted by the

government." *Id.* (original emphasis). It was because "plaintiffs only suspected that such interceptions had occurred" that such an allegation was "too speculative to support standing." *Id.*

The District Court below, however, missed the substantive difference between the *Clapper* plaintiffs' speculation that their information *would be taken*, and the reality that Appellants' information had *already been taken*. In *Beck* and *Watson*, as in both *Remijas* and *Adobe* and in contrast to *Clapper*, there was "no need to speculate" on the occurrence exposing plaintiffs to the risk of harm. *Remijas* at *12; *see also Adobe* at *27 ("in contrast to *Clapper*, . . . here there is no need to speculate as to whether Plaintiffs' information has been stolen"). The District Court, however, did not make this distinction, or properly consider that in both *Beck* and *Watson* the loss of personal information was not "speculative" as it had already been stolen.[1] *See* JA1049, 1091-1092. The five-step "speculative chain of possibilities" cited by the District Court as insufficient to support standing, *id.*, is

[1] In *Beck*, Defendants' formally chartered Administrative Investigation Board ("AIB") concluded in its official report that the laptop containing the personal information had been "stolen." JA824. Yet, Defendants continue to argue that the device is merely "missing" and Appellants assume a similar argument will be made regarding the "missing" boxes paper records in *Watson*. JA921-922, 928-931, 935, 937, 953. Such litigation positions should not be afforded any weight, especially when they are directly contrary to the unchallenged record evidence. *See, e.g., Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 213 (1988) (no deference to "an agency's convenient litigation position").

not found in this record. Indeed, the *Remijas* and *Adobe* courts found that the theft of personal information by a thief targeting such information, without more, establishes a sufficient likelihood of misuse to provide Article III standing. *Remijas* at *12; *Adobe* at *28. Thus, the District Court's analysis was unsound, as it was based on a misapplication of *Clapper*.

Further, both the *Remijas* and *Adobe* courts found that it was also not speculative to assert that the data thieves intended to misuse the personal information. *See Remijas* at *12 ("Why else would someone break into a store's database and steal consumers' private information?"); *see also Adobe* at *28 (hackers deliberately targeted Adobe's servers for personal information). Indeed, "the threatened injury here *could only be more imminent if Plaintiffs could allege that their stolen personal information had already been misused*." *Adobe* at *28 (emphasis supplied). The *Adobe* Court found – and the Seventh Circuit agreed – that under such circumstances, requiring plaintiffs "to wait for the threatened harm to materialize in order to sue would create a different problem: the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not fairly traceable to the defendant's data breach." *Remijas* at *12 (quoting *Adobe* at *28 n.5) (internal

quotation marks omitted). Indeed, Defendants here have already made such a traceability argument. *See, e.g.*, JA935, 956, 962.

In addition, while the District Court nodded to the "national security concerns" at play in *Clapper*, it failed to acknowledge the *separation of powers* issue raised by allegations "that other branches of government were violating the Constitution." *Adobe*, 2014 U.S. Dist. LEXIS 124126 at *25. Yet, this was the specific proposition for which the Supreme Court cited *Clapper* in a later opinion. *See Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (citing *Clapper* for the proposition that the "law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches."). Recognizing this issue, the Seventh Circuit characterized the *Adobe* court as having "persuasively applied" the principles of *Clapper* in being "reluctant to conclude that *Clapper* represents the sea change" in Article III jurisprudence because of the "sensitive context" of a case involving alleged Constitutional violations by other branches of the government. *Remijas* at *11; *see also Adobe* at *26 ("The U.S. Supreme Court itself noted that its standing analysis was *unusually rigorous* as a result." (emphasis supplied)). The *Adobe* Court declined to apply the same level of scrutiny to a case not involving such issues, finding instead that existing standards for finding Article III

standing in data theft cases remained good law. *Adobe* at *27 (because "nothing in *Clapper* reveals an intent to alter established standing principles, the Court cannot conclude that *Krottner* has been effectively overruled"). Thus, the District Court failed to properly consider the extraordinary context within which the Supreme Court intended *Clapper* to apply.

The District Court below thus erred in (1) concluding that *Clapper* established a new threshold for establishing Article III standing and (2) failing to distinguish cases where data has already been stolen from *Clapper's* speculative future theft.

D. The District Court Improperly Required Current Damages To Find Future Damages

To recover for the future consequences of an injury, the evidence must establish to a "*reasonable certainty*" that the future consequences will actually occur. *Id.* at *36. "An injured party is entitled to recover *all* damages, present and prospective, which are naturally a proximate consequence of the wrongful act." *Juaire v. United States*, 2012 LEXIS 19979 (Feb. 16, 2012) at *35 (Wooten, J.) (citing *Watson v. Wilkerson Trucking Co.*, 244 S.C. 217 (1964)) (emphasis supplied). To recover for the future consequences of an injury, the evidence must establish to a "*reasonable certainty*" that the future consequences will actually occur. *Id.* at *36. Although discussed at the January 28, 2015, hearing, *see* JA1004-1006, the District Court erroneously required concrete evidence that

Appellants' personal information had *already* been misused to find Article III standing to pursue damages for *future* harm. *See* JA1055 ("Plaintiffs have provided no evidence showing an intent or an attempt to misuse their personal information"); JA1091 (*Watson* Order at 18) ("Plaintiff has not alleged that there has been any actual or attempted misuse of her personal information, there is no injury at this time.").

As such, the District Court required, not a showing of a "threatened" or "imminent" future injury, but a showing of an injury that had already occurred. In doing so, the District Court not only misapplied the controlling law as discussed above, but also the long-established principles of future damages. This is particularly significant omission because the future damages standard of "reasonable certainty" is strikingly similar to the "reasonable risk" standard which the Secretary certified was satisfied on these facts as discussed below. 38 C.F.R. § 75.116.

Moreover, the District Court created the specific "problem" warned of by the Seventh Circuit. The District Court's decision forces Appellants "to wait for the threatened harm to materialize in order to sue" and handing defendants the argument "that the identity theft is not fairly traceable to the defendant's data breach." *Remijas* at *12 (quoting *Adobe* at *28 n.5) (internal quotation marks

omitted); *compare id., with* JA935, 956, 962 (Defendants traceability argument) *and* JA1067 ("Plaintiff Gajadhar has failed to show any connection between the laptop theft and the fraudulent charges" that she reported). There is no basis in the law to force individuals victimized by VA data breaches to have their finances ruined or their identities stolen before seeking relief as the District Court concluded.

E. The District Court Improperly Speculated On The Reasons For The Theft

Contrary to the approach by the *Remijas* and *Adobe* courts, the District Court below relied, at least in part, on its own speculation. "[O]ne must first *assume* that the computer was, in fact, stolen with the intent to misuse the personal information stored on it, not to simply pilfer the hardware." JA1058 (emphasis supplied). The record, however, establishes that no such assumption is required.

First, Defendants' own formally appointed investigation board unequivocally found that the laptop containing Appellants' personal information was "stolen." JA824. The record also establishes that the laptop had been installed for at least 6 years. JA823. The record contains no basis to speculate that anyone would risk federal prison to steal a more than 6-year-old laptop for its hardware value. Indeed, there is no suggestion, much less evidence, that such an aged and outdated device would have any monetary value as stolen property.

Moreover, this particular device was kept in a central room on the fifth floor of a federal medical facility with security personnel and access control. A thief did not just stumble onto this laptop. *Contra, e.g., In Re SAIC Backup Tape Data Theft Litig.*, 45 F.Supp.3d 14, 19 (D.D.C. 2014) (thief took GPS system and stereo along with data tapes from car in parking garage); *Randolph v. ING Life Ins. And Annuity Co.*, 486 F.Supp.2d 1, 2 (D.D.C. 2007) (laptop with personal information stolen during burglary of home). Thus, contrary to the District Court's speculation, anyone having knowledge of the laptop in the pulmonary lab would also likely be aware the type of personal information stored on it and have a plan for its (mis)use. *See Remijas* at *12 ("Why else would someone break into a store's database and steal consumers' private information?"). In any event, the District Court did not identify anything in the record as a basis for its speculation on the thief's intentions and to speculate on them was prejudicial legal error.

F. The District Court's Conclusion Regarding The Risk Of Future Harm Is Contrary To The Record

Even if *Clapper* substantively changed Article III standards, the District Court's finding that Appellants "failed to show that there is a 'substantial risk'" of future harm from the theft of their personal information cannot be reconciled with the record. To the contrary, the record establishes that: (1) there are significant risks from such data breaches, JA740 ("33%: Percent of health-related data breaches

that result in identity theft."); (2) Defendants expend tens of millions of dollars each year trying to avoid and mitigate those risks, JA749-750, and (3) the Secretary made a determination that the theft of laptop (*Beck*) and boxes of documents (Watson) were data breaches required providing credit monitoring because of a reasonable risk of harm to those victimized. JA25-27, 195-197. There was also expert testimony and submissions consistent with that record and supporting the Secretary's determination. JA227-230, 244-246, 849-873. The District Court's conclusion, therefore, is contrary to the record.

The District Court did not attempt to reconcile its contradiction of the Secretary's formal determination of "reasonable risk" to Appellants from the data breaches. Federal regulations require VA to, *inter alia*, respond to a data breach and perform a risk analysis of that breach. *See generally* 38 C.F.R. §§ 75.111-119. One explicit requirement is that the Secretary formally certify that "a *reasonable risk* for the potential misuse of sensitive personal information . . . exists" before expending federal funds on mitigation actions (e.g., credit monitoring). *Id.* § 75.116(a) (emphasis supplied). In addition, the Secretary is required to "take responsive action as specified . . . based on the *potential harms to individuals* subject to a data breach." *Id*. (emphasis supplied). The Secretary authorized credit monitoring following the loss of the laptop (*Beck*) and boxes of documents

(*Watson*). JA25-28, 195-197. The Secretary thus determined that Appellants were at "reasonable risk" of identity theft as a result of the Dorn data breaches, as a matter of law.

Yet, the District Court did not reconcile the Secretary's official certification of risk of future harm with the Court's conclusion that there was not sufficient risk to provide standing to seek relief for that same harm. As such, the District Court's analysis is, at best, incomplete. *See Remijas* at *14 ("It is telling . . . that [defendant] offered one year of credit monitoring and identity-theft protection . . . It is unlikely that it did so because the risk is so ephemeral that it can be safely disregarded."). In this case, the Secretary's decision to expend federal funds makes it similarly "unlikely" that the risk was ephemeral.

Further, Appellees' own (pre-litigation) determination was that loss of personal information results in a risk of "significant financial damage." In an email disseminated to Dorn employees on April 25, 2013, by the Information Security Officer, VA explicitly provided that "33% Percent of health-related data breaches that result in identity theft" and that "Every single piece of personally identifiable information represents a Veteran. JA739-741. If stolen, it can be used to *inflict significant financial damage* on him or her." JA740. In addition, VA officials testified that every single piece of personally identifiable information can be used

to inflict significant financial damage on the affected veterans. *See, e.g.*, JA96, 158-159, 163-174. These officials also conceded that the veterans whose information was compromised would be at an increased risk of having their identity misused. JA69, 96, 172-173. Taking these officials at their words, nearly 2,500 veterans are almost assuredly going to suffer *significant financial damage* because of the 2013 Dorn event alone and nearly 1,000 more because of the lost boxed records.

In addition, the testimony of Appellants' expert on identity theft and its associated costs to victims was supports Defendants' pre-litigation representations.

> [I]n 2008, consumers who received a data breach notification were *three times as likely* to go on to become a victim of actual identity theft/fraud. In 2009 the ratio rose to *four times*, followed by a *six-times* ratio in 2010. In 2011, among those receiving a data breach notification the fraud rate was *9.5 times* that of everyone else.

JA850. This testimony was, in turn, consistent with the evidence in other similar cases. *See, e.g., Ruiz v. Gap, Inc.*, 622 F.Supp.2d 908, 913 (N.D. Cal. 2009) *aff'd*, 380 F. App'x 689 (9th Cir. 2010) (claimant's expert opined that there was a four-to-one general increased likelihood that a data breach will lead to actual fraud victimization); *Perkins v. VA*, No. 2:07-cv-00310-IPJ, Dkt. No. 72, at 5-6 (N.D. Ala.) (quoting March 28, 2007, letter from the Centers for Medicaid and Human Services to VA Assistant Secretary for Office of Information and Technology

stating that "there is *a high risk* that the loss of personally identifiable information may result in *harm to the individuals* concerned." (emphasis supplied)).

The District Court, however, made only a passing reference to the April 25, 2013, VA document and Appellants' expert's conclusion, characterizing both as "based on a degree of speculation." JA1060. The District Court provided no basis for this conclusion and none is apparent in the record. In any event, contrary to the District Court's characterization, conclusions of future harm based this consistent and well founded information is much less speculative than the Court's conclusion regarding the thief's motivation and plans for the stolen laptop. Moreover, the District Court did not reconcile its conclusion of insufficient risk of harm with the Department's huge continuing expenditures to prevent and mitigate the very risk to which Appellants are now exposed.[2]

G. Appellants Have Standing For Their Administrative Procedure Act Claims Under That Statute's "Adversely Affected" Standard

The Administrative Procedure Act provides Appellants with a right to require VA to perform the safeguards actions "established" pursuant to the Privacy Act. A reviewing court shall "compel agency action unlawfully withheld or unreasonably

---

[2] The District Court's conclusion begs the question of why VA – and public companies and financial institutions – make any effort to protect citizens' personal information, much less spend millions upon millions of dollars to do so, when there is purportedly *no reasonable possibility of harm* from such data breaches.

delayed." 5 U.S.C. § 706(1); *Norton v. Southern Utah Wilderness Alliance*, 542 U.S. 55, 62 (2004). Congress provided such a review to "a person suffering legal wrong because of agency action, or *adversely affected* or aggrieved by agency action." 5 U.S.C. § 702 (emphasis supplied). Although "adversely affected" is not defined in the Administrative Procedure Act itself, the Privacy Act provides useful examples in the context of this case.

> [E]stablish 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). Thus, "substantial harm," "embarrassment," "inconvenience," and "unfairness" are all "adverse effects" to which individuals so "adversely affected" can maintain an Administrative Procedure Act claim for violation of the Privacy Act.

The District Court, however, again required more than a showing that Appellants were "adversely affected" by Appellees' actions and inactions to find standing. The District Court "agree[d] with Defendants" that "Plaintiffs lack standing because they fail to prove 'that, absent entry of injunctive relief by the Court, they will suffer *substantial* and immediate irreparable *injury*.'" JA1062,

1094 (emphasis supplied). This conclusion, however, is legally and factually adrift.

In essence, the District Court wrongly determined that "suffer[ing] substantial . . . injury" was the only way of being "adversely affected." "Substantial harm," however, is only one of the "adverse effects" that Privacy Act safeguards are required to protect against. 5 U.S.C. § 552a(e)(10). And, the record establishes Appellants have asserted being "adversely affected" by the failures of those safeguards in other ways. *Compare, e.g.*, JA336-337 (repeatedly checks credit reports because of unauthorized purchases), *with* 5 U.S.C. § 552a(e)(10) ("embarrassment," "inconvenience"), and JA972-972, 999-1000 (Appellants experienced worry, expenses for credit monitoring, fear of identity theft, frequent monitoring of accounts), *with* 5 U.S.C. § 552a(e)(10) ("inconvenience," "embarrassment," "unfairness"). Thus, Appellants were "adversely affected" by Appellees' actions and inactions and that is all that is required for standing under the Administrative Procedure Act. 5 U.S.C. § 706.

Moreover, these are the same "adverse effects" which *Chao* established "satisf[y] the injury-in-fact and causation requirements of Article III standing" under the Privacy Act. 540 U.S. at 624. This is not serendipity. To the contrary, the same acts which violate and provide standing under the Privacy Act, but for

which that Act does not provide adequate equitable relief, logically *should* provide standing under the Administrative Procedure Act. *See* 5 U.S.C. § 704 ("final agency action for which there is no other adequate remedy in a court are subject to judicial review"); *see also* 5 U.S.C. § 552a (no relief provided for "embarrassment," "inconvenience," and "unfairness"). The District Court's contrary conclusion was prejudicial legal error.

Further, the District Court's conclusion that "past Privacy Act violations are insufficient to establish Plaintiffs' to seek injunctive relief" is also factually defective. As discussed in detail below, the record establishes that not only has Dorn *never* been in full compliance with Privacy Act requirements, *no* VA medical facility has *ever* been in full compliance with that Act, which was first enacted in *1974*. There is, therefore, no factual basis upon which to rest a conclusion that the "past exposure to illegal conduct is insufficient to show that a present case or controversy exists," in this case. *Contra* JA1064, 1096 (citing *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983)).

To the contrary, on the record in this case, *Lyons* supports Appellants' position. Mr. Lyons challenged the use of "strangleholds" by police, but the *Lyons* Court rejected the theory that Mr. Lyons "need only be stopped for a traffic or other violation to be subject to strangleholds." *Lyons*, 461 U.S. at 107-108.

> But even assuming that Lyons would again be stopped for a traffic or other violation in the reasonably near future, it is *untenable to assert*, and the complainant made *no such allegation*, that strangleholds are applied by the Los Angeles police *to every citizen* who is stopped or arrested *regardless of the conduct of the person* stopped. We cannot agree that the "*odds*" that Lyons would not only again be stopped for a traffic violation but would also be subjected to a chokehold without any provocation whatsoever are *sufficient to make out a federal case for equitable relief*. We note that five months elapsed between [the event] and filing of the complaint, yet *there was no allegation of further unfortunate encounters* between Lyons and the police.

Id. at 108 (internal citation omitted) (emphasis supplied). The District Court's reliance on *Lyons* was misplaced for several reasons.

First, it is *not* "untenable to assert" on *this* record, and Appellants *have* alleged, that VA's inadequate actions and inactions will repeatedly harm *every* veteran regardless of anything those individuals can do. Dorn has *never* been in compliance with the Privacy Act. JA141 (never "full basic compliance"). Indeed, "as of 2013, there was *not one* single VA medical center that was fully compliant" with Privacy Act requirements. JA142. Contrary to *Lyons* and the District Court's conclusion, on this record and after 40 years of failing to achieve compliance, the only "untenable" assertion is that VA will adequately safeguard veterans' personal information going forward, without the relief Appellants seek. Thus, *Lyons* is fundamentally distinguishable.

Further, the "odds" of a future VA data breach, even if limited only to Dorn, are indistinguishable from certainty. Not only is there no factual basis to believe VA will ever achieve compliance with safeguards requirements left to its own devices, a VA official unequivocally admitted in the wake of the 2013 Dorn event that *"[t]hese occurrences are going to happen. It goes on throughout the VA."* JA44 (emphasis supplied). Indeed, several Appellants have already "beaten the odds," having been victims of at least two admitted VA data breaches, with Ms. Watson being victimized at least 3 times.[3] No such record supported Mr. Lyons.

Finally, and fundamentally distinguishing *Lyons*, there have been a host of "further unfortunate encounters." The record establishes that there were at least 17 *reported* data breaches at Dorn alone during the short period between the *Beck* laptop theft and the close of discovery, including the *Watson* records event. JA1063-1064. The facts that the *Lyons* Court found dispositive, therefore, simply do not exist here and, thus, the District Court erred in resting its decision on that case.

---

[3] All Appellants were victims of the 2006 lost laptop event which was reported to involve the personal information of approximately 26 million individuals, including all then-living veterans. *In re VA Data Theft Litig.*, 653 F.Supp.2d 58 (D.C.D.C. 2009). Several Appellants also received VA notification of the breach of their personal information as a result of the *Beck* event. Ms. Watson received VA notification of both the *Beck* and *Watson* events.

In sum, the District Court erred in failing to apply straightforward standing and future damages law. It also failed to distinguish *Clapper* and wrongly considered that case as establishing a new threshold for standing in data breach cases where the breach has already occurred. Similarly, the District Court failed to identify the dispositive factual differences between this record and the factual underpinnings of *Lyons*. The District Court's conclusion that Appellants lack Article III standing is, therefore, properly set aside.

II. Enforcement of Specific Agency Duties Is A Proper Exercise of Judicial Authority

The District Court's conclusion that "the APA does not provide for the broad judicial oversight that Plaintiffs seek," JA1068, is incorrect. Plaintiffs seek (1) only to ensure compliance with specific *existing* legal duties that *VA* has *already determined* necessary to adequately comply with Privacy Act requirements with (2) judicial oversight limited to review of VA's *own* measurement of its compliance, against its *own* standards, and as produced by its *own* processes for conducting such assessments. Such relief is not fairly characterized as "broad judicial oversight" and, to the contrary, is well within the scope of relief authorized by the Administrative Procedure Act.

Moreover, Appellants do not dispute that the Administrative Procedure Act cannot be used to tell VA what to do or how to do it. And, they are not seeking to

do so. Once VA has determined what needs to be done and how it is to be done, however, Appellants can use the Administrative Procedure Act to compel VA to do what it said had to be done.

A. The Identified Requirements Have The Force Of Law

VA implements its Privacy Act requirements through a myriad of rules, policies, procedures, and other guidance that mandate actions. If an "agency's decision and the processes authorized to make that decision resemble legislative decisions and legislative processes, the agency stands in the shoes of Congress, and its decisions carry the force of law." *A. T. Massey Coal Co. v. Barnhart*, 472 F.3d 148, 166 (4th Cir. 2006); *see also Diebold v. United States*, 947 F.2d 787, 790 (6th Cir. 1991) (finding that a "circular" establishing a "mandatory" process was reviewable under the Administrative Procedure Act); *W. Va. Highlands Conservancy v. Norton*, 190 F.Supp.2d 859, 867 (S.D.W. Va 2002) ("Regulations promulgated by an agency under the authority of the general statute also provide sufficient law for a court to apply."). Removing all doubt regarding the "force of law" of the VA policies and directives applicable in this case, VA Directive 6502 explicitly ties compliance with applicable guidance to Privacy Act compliance:

> VA shall comply with current laws and regulations. VA shall evaluate legislative and regulatory proposals involving the collection use, and disclosure of PII, and shall continually assess compliance with all applicable Federal privacy laws and regulations. All VA entities that maintain PII shall:

> (1) Identify the [personal information] for which they are responsible;
>
> (2) Comply with all extant and future Federal privacy law, regulations, and guidance pertaining to that [personal information].

JA45. VA Directive 6502, in turn, itself references *47* statutes, regulations, directives, and other documents for which VA asserts it maintains compliance through other VA policies, procedures, and guidance. JA46-49. Thus, the requirements at issue in this case had the force of law when they were violated.

B. Creation of Requirements Alone Does Not Satisfy Privacy Act Duties To Safeguard Personal Information

The Privacy Act requires VA to actually safeguard personal information, not just *promise* to safeguard personal information. The Privacy Act is particularly specific in the types of, and purposes for, the safeguards it requires.

> [E]stablish 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). Appellants contend that merely paying lip service to the Privacy Act by "establishing" requirements for these safeguards but not implementing those requirements, is precisely the type of wrong that the Administrative Procedure Act was intended to right.

Where the rights of individuals are affected, it is incumbent upon agencies to follow their own procedures. *Morton v. Ruiz*, 415 U.S. 199, 235 (1974). This has

long been so even where the agency's internal procedures are possibly more rigorous than otherwise would be required. *Id.* (citing *Service v. Dulles*, 354 U.S. 363, 388 (1957); *Vitarelli v. Seaton*, 359 U.S. 535, 539-540 (1959)). Thus, VA must abide by its procedures, e.g., Directive 6502, to claim compliance with the laws cited as being satisfied by those procedures.

Removing any doubt in this case, Congress was explicit that VA actually had to comply with the Privacy Act procedures that it created.

> The Secretary *shall ensure* that the Department information security program includes the following elements:
> . . .
> (3) Selection and *effective implementation* of minimum, mandatory technical, operational, and management security controls, or other compensating countermeasures, to protect the confidentiality, integrity, and availability of each Department system and its information.
> . . .
> (7) A process for planning, developing, *implementing*, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices.

38 U.S.C. § 5722(b)(3), (7) (emphasis supplied); *see also id.* § 5723(9). Thus, to the extent that the District Court impliedly agreed with Appellees that the Privacy Act does not require VA or its officials and employees to actually *implement* the procedural requirements to safeguard personal, *see* JA1034-1035, it was legal error.

C. Dorn VA Medical Center Has Never Been In Compliance

The District Court's conclusion that Appellants' "plea for injunctive relief hinges on the VA's *previous* Privacy Act violations," JA1067, is an erroneous reading of Appellants' allegations and the record. The danger of *another* injury from Dorn's failure to safeguard is not "conjectural" or "hypothetical" because Dorn has *never* been fully compliant with VA privacy procedures. *See* JA141. Indeed, "as of 2013, there was *not one* single VA medical center that was fully compliant" with Privacy Act requirements, JA142, and another VA official stated that "[t]hese occurrences are going to happen. It goes on throughout the VA." JA44.

Moreover, not only was Dorn not in "full" compliance in 2013, the official AIB Report documents extensive failures in *every* category of Privacy Act safeguards. As discussed below, these deficiencies generally (1) had existed for years and (2) were known to Appellees, and those that were not known (3) would have been known if they had properly monitored compliance. Yet, as the Dorn Privacy Officer stated, at the time of the Dorn event:

> They did not secure the patient information. They left doors unlocked. They just completely disregarded any respect for privacy. There's just so many, there's just so many issues. I believe that they violated – there's just so many issues dealing with privacy. . . . Like I said it was a privacy, not just a privacy issue, it was a security issue also because the doors were

> unlocked. There was no, there was no – *they did not make any initiative to protect the veterans' personal information*.

JA814-815 (emphasis supplied). In other words, there were *no* effective technical, physical, *or* administrative safeguards were in place when the laptop was stolen in direct violation of myriads of statutory, regulatory, and procedural duties.

1. Appellees Violated VA Technical Safeguards Requirements.

Defendants ignored mandatory VA directives to encrypt *all* laptop computers containing PII. A November 15, 2011, VA Memorandum from the Assistant Secretary for Information and Technology identified the need for encrypting "*all* VA government-owned laptops" by February 29, 2012. JA839 (original emphasis). The memo noted that "VA laptops have been compromised both from within VA's protective environment and from outside VA's boundaries." *Id.* Yet, the Dorn Chief of Biomedical Engineering stated that he did not order the laptop encrypted. JA798-799. The VA Director of Field Security testified that Dorn did not comply with VA requirements to encrypt the laptop, JA150, 151-152, 181, and that Dorn had even failed to inventory the laptop as required by VA policy. JA191.

2. Appellees Violated VA Physical Safeguards Requirements

Appellees erroneously *assumed* – without confirming – that the missing laptop "was stored in a locked room with restricted/managed access control." JA830. As

determined by the AIB, however, the room from which the laptop was stolen was *not* locked and there were *no* effective access controls. JA823-824. Moreover, Dorn routinely (1) issued "master" keys instead of "change" keys to employees, thus giving essentially unfettered access to the entire facility rather than only specific spaces[4] and (2) failed to change the locks in the area where the laptop was stored for at least *three years* despite reports of missing keys and numerous personnel changes despite a requirement that "the key cores operable by the lost key will be changed and all affected keys replaced *within five days*." JA848 (emphasis supplied).

The record also makes clear that prior to the theft, Appellees did not even implement the most basic safeguard of requiring a password to access the personal information on the missing laptop. JA788-789, 803. The laptop operator stated that he would turn on the laptop in the morning and work on it all day without entering a password. *Id.* Thus, anyone could walk into the unlocked room and, if choosing to not take the computer entirely, could page through its personal information unhindered by a password or encryption.

---

[4] This practice was widely known and apparently an accepted practice. *See* JA828 ("practice here of issuing master keys instead of change keys will take the integrity out of a keying system"); JA804 ("everyone in respiratory has keys to my office, Al's office and Randy's. It's a standard key that fits almost everything.").

Finally, "the laptop also *should have been cabled*" to a secure fixture. JA784 (emphasis supplied). Yet, VA's Director of Field Security testified that Dorn was not in compliance with VA requirements for a cable lock to be installed on laptop computers. JA773. Neither the stolen laptop nor the other computers in the same area were secured by locking cables or any other security devices. JA794, 805-806. Indeed, the missing "laptop was *only attached via a Velcro strip, no cabling*." JA824; *see also* JA794 ("The only thing that connected it was a piece of double stick Velcro"). This was in direct violation of a Dorn memorandum on "Reasonable Privacy and Security Safeguards," which stated that "Staff *shall lock* down" computers when not in use. JA837.

3. Appellees Violated VA Administrative Safeguards Procedures

Dorn's "administrative" safeguards were largely detailed in the "Reasonable Privacy and Security Safeguards" section of Medical Center Memorandum 544-1023 "Privacy Policy." JA825. This document explicitly stated that "*[a]ll members of the workforce are responsible* for complying with this privacy policy, applicable federal laws and regulations, [VA] regulations and policies, Veterans Health Administration (VHA) policies, as well as the procedures and practices developed in support of these policies." JA831; *see also* JA825 ("All facility workforce members shall ensure that appropriate administrative, technical, and

physical safeguards are used"). Further, the Dorn "Executive Management (Medical Center Director, Associate Director, Chief Nursing Executive, Chief of Staff) is responsible for," among other things, "ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation (e.g., . . . Privacy Rule (45 C.F.R. Parts 160 and 164), the Privacy Act (PA) [5 U.S.C. 5701]"). JA832.

Dorn managers and employees were ignorant of any mandatory safeguards procedures. For example, the Dorn Chief of Engineering did not remember seeing a critical memorandum from the Director of Health Care Technology Management discussing relevant requirements. JA809-810. Dorn also ignored, or at least failed to adequately implement, numerous VA requirements to identify, track, and physically inventory equipment. JA841-847. When asked how many "biomedical laptops" there were in Dorn similar to the stolen device, the Dorn Information Security Officer stated that he could not provide an exact number. JA822. In response to an investigator who found it "hard to believe or kind of surprising that a piece of equipment could possibly have been brought into the facility skipping the whole receiving process possibly by a vendor straight to a service line," the Dorn Chief of Logistics unequivocally stated: "Unfortunately *I know for a fact that happens*." JA785-786.

D. The Non-Compliance Is Systemic, Longstanding, And Known To Management

Nor are these isolated failures or caused by an occasional inattentive employee, which courts have found do not rise to agency failures. *See Thompson v. Dep't of State*, 400 F.Supp.2d 1, 23 (D.D.C. 2005) (agency employee left investigation report on plaintiff's office chair); *Alexander v. FBI*, 691 F.Supp.2d 182, 192 (D.D.C. 2010) (FBI provided plaintiffs information in response to "facially ordinary requests submitted according to unchallenged procedures that had been in place for thirty years"); *White v. Schafer*, 738 F.Supp.2d 1121, 1142 (D. Colo. 2010) (plaintiff focused "on one instance in which [Privacy Act] safeguards proved ineffective."). Plaintiffs submit that after almost five decades to implement the organic requirements that *not a single* VA medical facility is compliant with Privacy Act is exactly the type of habitual agency inaction from which the Administrative Procedure Act was enacted to provide relief and the District Court erred in concluding otherwise.

Thus, the District Court's conclusion that Appellants "do not have standing to seek injunctive relief pursuant to the [Administrative Procedure Act]" is not supported by the record. On this record, the conclusion that is "conjectural" and "hypothetical" is the District Court's conclusion that Appellants' information will not again be lost by or stolen from Dorn. *Contra Lyons*, 461 U.S. 95 at 101-102.

Indeed, not only is the District Court's conclusion without factual basis in the record, it is *contrary* to the record.

E. The District Court Has Authority To Provide The Requested Relief

The District Court's conclusion that "Defendants are entitled to summary judgment on Plaintiffs' [Administrative Procedure Act] claim because the [[Administrative Procedure Act] does not provide for the broad judicial oversight that Plaintiffs' seek, JA1068, is not supported by the law. Two United States Court of Appeals for the District of Columbia Circuit decisions contain detailed discussions of a District Court's authority to order mandatory equitable relief against a federal agency. *See Cobell v. Norton*, 392 F.3d 461 (D.C. Cir. 2004) (upholding order for agency to complete remedial plan, as modified) and *Cobell v. Norton*, 240 F.3d 1081 (D.C. Cir. 2001) (upholding injunctive relief because it allowed agency which acted unlawfully to retain "discretion to determine in the first instance" how to bring themselves into compliance.). Although the District Court requested this case law, JA991-992, its opinions do not discuss them. *See generally* JA1038-1073, 1074-1097.

Both cases involve long-running litigation between the United States Department of the Interior and several Native American organizations seeking an accounting of funds held in trust by the United States for individual Native

Americans. In the first decision, the Circuit Court discussed the duties owed to the plaintiffs and Interior's "historical record of recalcitrance" to comply with its statutory duties towards plaintiffs. *Cobell v. Norton*, 240 F.3d at 1098-1108. The Circuit Court then analyzed the relief ordered by the District Court, including *the promulgation of regular reports and updates to the court while it retained jurisdiction*, and found that the "ordered relief is relatively modest." *Id.* at 1109.

> The level of oversight proposed by the district court may well be in excess of that countenanced in the typical delay case, but so too is the *magnitude of government malfeasance* and potential prejudice to the plaintiffs' class. *Given the history* of destruction of documents and loss of information necessary to conduct an historical accounting, the failure of the government to act could place anything approaching an adequate accounting beyond plaintiffs' reach. This fact, *combined with the longstanding inability or unwillingness of government officials* to discharge their fiduciary obligations, excuse court oversight that might be excessive in an ordinary case.

Id. (emphasis supplied). The Court also explicitly responded to the government's objections to the ordered relief.

> The government is correct that the court imposed continual reporting requirements that may be in excess of that which would be minimally required to discharge the government's duties. However, it *does not seem that the district court's remedies are disproportionate to the nature of the government's breach*. Moreover, while the court should (and did) remand to the agency for the proper discharge of its obligations, the court should not abdicate its responsibility to ensure that its instructions are followed. This would seem particularly appropriate where, as here, there is a record of agency recalcitrance and resistance to the fulfillment of its legal duties While a *court's retaining of jurisdiction of five years* may be unusual, federal courts regularly retain jurisdiction until a federal agency has

> complied with its legal obligations, and have the authority to compel regular progress reports in the meantime.

Id. (emphasis added) (internal citations omitted). In upholding the District Court's authority, the Circuit Court found ample precedent. *Id.* (citing *In re United Mine Workers of Amer. Int'l Union*, 190 F.3d 545, 546 (D.C. Cir. 1999) (retaining jurisdiction and requiring status reports pending completion of agency action); *Northern States Power Co. v. U.S. Dep't of Energy*, 128 F.3d 754, 760 (D.C. Cir. 1997) (retaining jurisdiction pending agency's compliance with court's mandate); *Air Line Pilots Ass'n, Int'l v. CAB*, 750 F.2d 81, 88-89 (D.C. Cir. 1984) (retaining jurisdiction and ordering periodic progress reports)).

Four years later, the *Cobell* Court reviewed another district court injunction. 392 F.3d 461. The Circuit Court again upheld "the requirement [for DOI] to submit a plan." *Id.* at 475. The Circuit did vacate the District Court's requirements that "directs [DOI], rather than plaintiffs, to identify defects in its proposal" and the language that subjected DOI to contempt charges, rather than APA civil remedies, for minor future violations, but did so because it found that subsequent legislation had removed the legal authority for the district court to require those actions. *Id.* at 464.

Appellants here seek equitable relief which the *Cobell* Court found within the boundaries of the Administrative Procedure Act and appropriate when an agency,

as here, has an "historical record of recalcitrance." *See, e.g.*, JA22 (praying for the Court to enjoin Defendants "until and unless Defendants demonstrate to the Court that adequate information security has been established pursuant to the applicable federal standards")); JA65 ("requesting an accounting of Privacy Act records"). The relief sought was also discussed during the January 28, 2015, hearing. *See* JA978 ("the equitable relief we seek here is for the court to maintain jurisdiction [and] order the Secretary to provide his own plan"); *id.* ("We are not asking [the court] to measure, we're not asking the court to decide when they need to do something, how they need to do it, what color it needs to be"); JA981 ("We want to try to get the problem fixed any way the VA wants to fix it.")); JA986 ("We're not asking for them to implement a security program, we're saying you said you needed locks"); JA991 ("We are not asking them for anything that they haven't said they are trying to do.")). *Cobell* establishes that the District Court has the authority to "retain jurisdiction until" VA "has complied with its legal obligations" and also has "the authority to compel regular progress reports in the meantime." 240 F.3d at 1109. The District Court's conclusion otherwise is incorrect and is properly vacated.

Moreover, this result does not conflict with *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55 (2004) ("*SUWA*"), as concluded by the District Court. A

plaintiff "cannot seek *wholesale* improvement of [a] program by court decree, rather than in the offices of the Department of the halls of Congress, where programmatic improvements are normally made." *SUWA*, 542 U.S. at 64 (original emphasis). Consistent with *SUWA*, Appellants have repeatedly stated that they do not want the District Court to require *any* changes in VA's program. *See, e.g.*, JA2-3, 7-11, 52, 55-59, 978-981, 986, 991. Indeed, Appellants only seek that VA "demonstrate to the Court" that it has "adequate information security" under either its current program or one of its own choosing. JA981, 990.

Further, the actions and inactions complained of are not subject to "programmatic improvement" because they *are discrete actions already required under the existing program*. As a simple example, VA's program already requires cable locks on laptop computers, JA773, but Dorn did not install a cable lock on the stolen laptop. JA773, 784. Plaintiffs do not seek to "improve" the program by a judicial fiat that VA must install cable locks because that requirement already exists. Appellants seek judicial oversight to ensure that VA installs cable locks on laptops *because VA's safeguards program already requires it*. In addition, it is an unreasonable reading of *SUWA* to conclude it commands seeking such discrete and specific relief "in the offices of the Department or the halls of Congress" because the requirement to use a cable lock *already exists*, as does a specific requirement

for each of the discrete actions and inactions complained of by Appellants (*see* above discussion of safeguards deficiencies). Indeed, the absurdity of seeking such relief from Congress further illustrates just how narrow and specific the actions Appellants seek to compel are. *Contra* SUWA at 66-67 (discussing examples of "broad programmatic" changes).

CONCLUSION

In sum, Appellants have Article III standing to pursue their Privacy Act claims and seek the equitable relief they seek under the Administrative Procedure Act. The District Court erred by reading too much into *Clapper* and failed to properly distinguish *Lyons*. As a result, the District Court erroneously required a showing of much more than "adverse effects" to establish standing for individuals "adversely affected" by the identified data breach incidents. Thus, the District Court has authority under the Administrative Procedure Act to provide Appellants with the equitable relief because of the history of agency recalcitrance in failing to have ever established compliance with Privacy Act requirements.

MIKE KELLY LAW GROUP, LLC

BY: /s/ Brad D. Hewett
Brad D. Hewett
Fed. Id. No. 10388
D. Michael Kelly
Fed. Id. No. 2299
P.O. Box 8113
Columbia, SC 29202
803.726.0123 (tel)
803.461.2173 (fax)
mkelly@mklawgroup.com
bhewett@mklawgroup.com

And

Douglas J. Rosinski, Esq.
Fed. Id. No. 6995
701 Gervais St., Ste. 150-405
Columbia, SC 29201-3066
803.256.9555 (tel)
888.492.3636 (fax)
djr@djrosinski.com

Counsel for Appellants

Dated: August 10, 2015

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies that this brief complies with Fed. R. App. 28.1(e)(2) and Fed. R. App. P. 32(a)(5)(B).

This brief has been prepared in a proportionally spaced typeface (Times New Roman) using Microsoft Word in 14-point font and contains 12,400 words.

This 10th day of August 2015.

/S/ BRAD D. HEWETT

CERTIFICATE OF SERVICE

The undersigned, counsel of record for Appellants, hereby certify on this 10th day of August, 2015, that a true copy of the foregoing "Appellants' Brief" was filed with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit using the CM/ECF system which will send notification of such filing to the following CM/ECF participants:

Sonia K. McNeil
U.S. Department of Justice
950 Pennsylvania Avenue, NW, Room 7234
Washington, DC 20003
202.616.8209
sonia.k.mcneil@usdoj.gov
Counsel for Appellees

Mark B. Stern
U.S. Department of Justice
950 Pennsylvania Avenue NW, Room 7531
Washington, DC 20003
202.514.5089
mark.stern@usdoj.gov
Counsel for Appellees

/S/ BRAD D. HEWETT