What Happens to Information Stolen in a Data Breach and Why It Matters in Litigation

By: Joseph H. Wieseman and Alex M. Barfield
Hawkins Parnell Thackston & Young, LLP

Joseph H. Wieseman is a partner at Hawkins Parnell Thackston & Young, LLP, and concentrates his practice in business litigation and legal malpractice. He has successfully represented clients in matters involving intellectual property, data breaches, corporate governance, commercial contracts, and real estate. Joe has a wide range of litigation experience involving internal investigations, arbitrations, and mediations. He can be reached at jwieseman@hptylaw.com.

Alex M. Barfield has been with Hawkins Parnell Thackston & Young, LLP for nearly twelve years and is a partner in the firm's Labor & Employment Group. Alex represents management in labor and employment litigation, and also handles commercial litigation for corporate clients. His practice also includes litigation related to employment contracts, data breach liability, commercial collection, and the Fair Credit reporting Act. He can be reached at abarfield@hptylaw.com.

Within weeks of Sony's data breach in November 2014, multiple class actions had been filed.[1] With Home Depot's breach, the first class action lawsuit only took days.[2] While there are various incentives for attorneys and their clients to immediately file an action in the wake of a data breach, such hasty filings can illuminate a fundamental problem with their lawsuits. A defining factual issue in data breach lawsuits involves whether the breach resulted in the actual theft of an individual plaintiffs identity or simply an increased risk of identity theft in the future. In other words, a question exists as to whether the mere occurrence of a data breach, without more, can confer upon a plaintiff a cognizable injury, and thus the standing necessary to file a lawsuit. Absent that standing, a plaintiff simply cannot proceed.

This article will discuss how the *misuse* of stolen personal information from a data breach impacts subsequent litigation. As shown herein, federal courts have split on whether a future risk of identity theft constitutes a compensable injury for purposes of standing. Georgia courts have not expressly addressed this split in authority, but the present legal landscape tracks the existing majority view that an increased risk of harm

resulting from a data breach is not, in and of itself, a compensable injury.

I. The Business of Stolen Data and Notification Requirements

Experienced hackers have little problem monetizing stolen data. An obvious benefit to data as opposed to physical property is the speed and ease at which it can be exchanged over the internet. Whether the information is a name, address, date of birth, social security number, credit card number, or even a mother's maiden name, there is a thriving internet black market to buy and sell stolen data. Once purchased or otherwise transferred, the stolen data can then be used for its ultimate purpose: to commit identity theft. Fraudsters can clone credit and debit cards to purchase goods or prepaid credit cards. With a social security number and related personally identifiable information (PII), fraudsters can open lines of credit, take out loans, or even submit false tax returns.

Given the manner in which most high-profile identity theft is carried out, it is critical that affected individuals know their information has been compromised in a data breach. Only then will they know to take steps to protect themselves by reviewing bank statements and credit reports for suspicious activity.[3] As a result, the vast majority of states have breach notification laws requiring covered entities to notify affected individuals of a data breach.[4] The types of information and the entities required to comply vary from one state to the next. In an effort to address and preempt the patchwork coverage, the latest incarnation of uniform federal legislation for reporting data breaches, the Data Security and Breach Notification Act of 2015, is currently pending before Congress. Still, federal notification laws already exist for breaches concerning certain types of information—most notably protected health information (PHI).[5]

In Georgia, only certain entities are required by statute to notify impacted persons of a data breach.[6] The first is "data collector," which is defined as essentially any governmental agency.[7] The second is "information broker," which is defined as "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties ... ."[8] The plain language of the statute indicates it does not apply to most businesses, including those often associated with high-profile data breaches—retailers.[9]

Whether they are required to do so or not, businesses that notify customers of a data breach customarily have offered free identity theft protection services for a period of time (usually a year) following the breach.[10] The point of such notifications and monitoring services is to limit the chances of a fraudster using the stolen data to actually commit identity theft.

The notification and monitoring services result in a substantial number of individuals that have their information stolen in a data breach but do not actually suffer identity theft. An additional variable to consider is the unpredictability of the criminal underworld. For some unknown reason, a person's stolen credentials may not filter through the black market to someone with the skill, motivation, or opportunity to misuse it.

So where does that leave an individual whose information has been stolen in a data breach, but who has not been a victim of identity theft? This is an issue facing many litigants who hastily file lawsuits immediately following notice of a data breach. They are unable to allege they have actually suffered some cognizable form of identity theft. They instead allege the data breach has made them more likely to suffer identity theft in the future. In other words, they allege they have been injured through an elevated risk of future harm.

As demonstrated in the next section, the majority of courts that have considered this issue have held that an elevated risk of identity theft following a data breach does not constitute a sufficient injury to sustain a claim for relief. A minority position exists finding that an individual need not actually suffer identity theft before bringing a cognizable claim. So far, this issue primarily has played out in the context of standing in federal courts. Georgia courts have not generated significant authority on the issue, but, at present, appear to follow the majority view, as set forth below.

II. Article III Standing

Article III of the United States Constitution limits jurisdiction of federal courts to *cases* or *controversies*.[11] It is a threshold question in every federal case that must be determined at the time when the plaintiff files his complaint.[12] To establish Article III standing, a plaintiff must first demonstrate an injury in fact.[13] The injury in fact is an invasion of a legally-protected interest that is concrete and particularized.[14] The injury must be actual or imminent at the time the suit is filed and cannot be conjectural or hypothetical.[15] In addition to injury in fact, a plaintiff also must show a causal connection between the injury and the conduct complained of, as well as a likelihood that the injury will be redressed by a favorable decision.[16]

The seminal case on whether an increased risk of harm of identity theft is a cognizable injury is *Clapper v. Amnesty International USA*.[17] Prior to *Clapper*, various courts, including the Northern District of Georgia, found that the future risk of identity theft following a data breach was insufficient to prove injury in fact.[18] In siding with defendants, courts generally found the threat of future harm too speculative when it relied upon future acts of unknown third parties (i.e. hackers and fraudsters) to misuse the data to a plaintiffs' detriment.[19] Courts also have held that plaintiffs cannot claim mitigation expenses (e.g. out-of-pocket payments for credit monitoring) as an injury

absent some cognizable allegation of identity theft to show that such expenses were necessary.[20] On the other hand, the United States Courts of Appeals for the Seventh and the Ninth Circuits held that the risk of future identity theft was sufficient to establish an injury in fact.[21] In *Krottner v. Starbucks Corporation*, the Ninth Circuit found a "credible threat of real and immediate harm" after a company laptop with unencrypted PII had been stolen despite there being no allegation that any PII had been misused.[22] The *Krottner* court made no findings with respect to the role of third parties actually misusing the stolen data. The mere fact that the laptop had been stolen was sufficient in and of itself to constitute an imminent risk of harm.[23]

Clapper was actually not a data breach case and did not involve issues of identity theft. Instead, *Clapper* concerned an amendment to the Foreign Intelligence Surveillance Act (FISA).[24] The amendment authorized government surveillance of individuals who were not "United States persons" and believed to be located outside the United States.[25] Respondents, who engaged in communications with potential targets, filed suit on the day FISA was amended (i.e. before any communications were intercepted) challenging its constitutionality.[26] They alleged injury in fact based on the objectively reasonably likelihood that their communications with potential targets would be intercepted at some point in the future.[27] They also claimed injury because they had already taken costly and burdensome measures to protect the confidentiality of their communications.[28]

In rejecting the first ground, the Court stated that the threatened injury must be "certainly impending to constitute injury in fact" and "allegations of possible future injury are not sufficient."[29] The Court found the respondents' "speculative chain of possibilities d[id] not establish that injury based on a potential future surveillance is certainly impending ..."[30] In reaching its decision, the Court highlighted its reluctance to endorse standing theories that rely on speculation about the decisions of independent actors.[31] With respect to the second ground, costs incurred to protect their communications, the Court rejected the respondents' attempt to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[32]

Echoing many of the points raised in the majority of courts finding no injury in data breach cases, the *Clapper* decision seemed destined to end the debate on whether an increased risk of identity theft could constitute an injury in fact. In *Strautins v. Trustwave Holdings, Inc.*, for instance, the district court reasoned that identity theft concerns depend on a number of variables involving third parties.[33] Like the Supreme Court's assessment in *Clapper*, the district court noted that identity theft depends on whether the stolen data was subsequently sold or transferred, whether anyone who obtained the data attempted to use it,

and whether or not he succeeded.[34] According to the district court, the plaintiffs' complaint in that case, which was "filed less than three weeks after the data breach ... provide[d] no basis to believe that any of these events have come to pass or are imminent."[35] Likewise, in *Peters v. St. Joseph Services Corp.*, the district court rejected the plaintiff's claims while pointing out that she could not describe her purported injury without beginning the explanation with the word "if".[36] She would be harmed in the future *if* third parties formed an intent misuse the stolen data and *if* they actually misused the data to commit identity theft.[37] Such threatened injury was not "certainly impending" as required to constitute an injury in fact.[38]

Notwithstanding *Clapper*, a minority number of courts has continued to recognize that an increased risk of identity theft following a data breach is sufficient to demonstrate an injury for purposes of standing.[39] The case of *In re Adobe Systems, Inc. Privacy Litigation* provides perhaps the most illuminating rationale for this conclusion.[40] In *Adobe*, hackers targeted Adobe's servers and spent weeks collecting customers' PII and personal financial information (PFI) as well as the company's proprietary source code. The district court stated there was no "need to speculate as to whether the hackers intend to misuse the personal information ...or whether they will be able to do so."[41] In support, the district court noted hackers intentionally targeted Adobe, and the stolen source code (but not customer PII or PFI) had already surfaced on the internet.[42] More tellingly, the district court highlighted the inherent difficulty for plaintiffs bringing suits under a future risk of identity theft. "[T]o require Plaintiffs to wait until they actually suffer identity theft ...in order to have standing would run counter to the well-established principle that harm need not have already occurred or be literally certain in order to constitute injury-in-fact."[43]

III. Georgia

Many high-profile data breach cases end up in federal court not because they involve federal questions.[44] Instead, jurisdiction is typically based upon the Class Action Fairness Act of 2005, which relaxed diversity requirements for class actions involving more than $5,000,000.[45] As a result, cases involving data breaches and future risk of harm should not be considered issues reserved solely for federal courts as they are based primarily on state law claims. Still, not too many data breach and identity theft cases have been addressed by Georgia's appellate courts. To date, no Georgia appellate court has expressly addressed the split in authority on the issue of increased risk of future identity theft in data breach cases. In fact, the issue of standing in Georgia state courts typically applies to constitutional challenges.[46] Still, as in Article III courts, Georgia law requires that a plaintiff suffer a cognizable injury in order to bring a claim.

The few cases that have dealt with the issue of future harm indicate that Georgia courts are more likely to

align with the majority view that increased risk of harm is not a sufficient injury to support a claim for relief. In *Finnerty v. State Bank & Trust Company*, a bank sued Finnerty for defaulting on a note.[47] Finnerty counterclaimed alleging, inter alia, negligence and invasion of privacy based on the bank's inclusion of his social security number in an exhibit to the complaint. He alleged that he suffered an increased risk of identity theft as a result of the public disclosure.[48] Based on Georgia law, the Georgia Court of Appeals reiterated that "a wrongdoer is not responsible for a consequence which is merely possible, according to occasional experience, but only for a consequence which is probable, according to ordinary and usual experience."[49] Finnerty failed to show the disclosure made it probable that he would suffer any identity theft or that any specific persons actually accessed his personal information and the Court of Appeals concluded that a "fear of future damages [was] too speculative to form the basis for recovery."[50]

In *Rite Aid v. Peacock*, a detective sued his former pharmacist for selling his information to a neighboring Walgreens pharmacy.[51] The Court of Appeals held that the detective had failed to prove any physical or financial injury, nominal or otherwise, flowing from the allegedly illegal sale of his information. In dicta, the Court of Appeals noted that "Peacock can only speculate that criminals he has had a hand in apprehending may associate with a Walgreens employee having access to his prescription information, given the absence of evidence that a Walgreens employee has harmed him ... by misuse of that information."[52] In line with the majority of federal courts, Rite Aid suggests not only is some actual injury required, but also speculation on the conduct of third-party criminals will not suffice.

Georgia cases not involving allegations of identity theft also may be helpful to an analysis of future harm in this context. For instance, the Supreme Court of Georgia affirmed a finding for the American Red Cross after the plaintiff failed to prove actual exposure to HIV following a blood transfusion.[53] Plaintiff's fear of exposure to the virus was insufficient to establish actionable damages suffered by the plaintiff.[54] In another case involving exposure to insecticide, the Court of Appeals held that the plaintiff was required to show an increased risk of developing cancer to a degree of "reasonable medical certainty."[55] Evidence that exposed children would require monitoring in the future was not sufficient to permit recovery of damages.[56]

IV. Conclusion

Outside of a minority of courts, litigants racing to the courthouse following a data breach will continue to face major obstacles in attempting to litigate their claims. While it may seem somewhat perverse to insulate businesses from accountability based on what hackers and fraudsters are able to do with stolen data, it would appear equally perverse to hold businesses accountable for a harm that may never materialize.

End Notes

[1] *See, e.g., Corona* v. *Sony Pictures Entm't, Inc.,* No. 2:14-CV-09600-RGK-SH (C.D. Cal. filed Dec. 15, 2014).

[2] *Solakv. The Home Depot, Inc.,* No. 1:14-CV-02856-TWT (N.D. Ga. filed Sept. 4, 2014).

[3] With the increasing number of data breaches reported, a phenomenon known as data breach fatigue has set in. At least one report indicates about a third of consumers notified that their information had been compromised in a breach took no action to protect themselves from fraud thereafter. Experian, 2015 Second Annual Data Breach Industry Forecast 3 (2015), available at http://www.experian.com/assets/data-breach/white-papers/2015-industryforecast-experian.pdf?ga=l.172114915.1943093614.1418003182.

[4] At the time of drafting this article, Alabama, New Mexico, and South Dakota were the only states without a breach notification law.

[5] Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 17932.

[6] O.C.G.A. § 10-1-912.

[7] O.C.G.A. § 10-1-911(2).

[8] O.C.G.A. § 10-1-911(3).

[9] *See id.*

[10] California recently amended its privacy laws to seemingly require monitoring services. Cal. Civ. Code § 1798.82(d)(2)(G) (Deering 2015). The section reads, "[i]f the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached…" Id. The "if any" language, however, arguably only mandates that such services be provided at no cost *if* offered rather than requiring an entity to provide identity theft protection services after every breach.

[11] *Hollywood Mobile Estates Ltd. v. Seminole Tribe of Fla.,* 641 F.3d 1259, 1264 (11th Cir. 2011) (citing U.S. Const.art. III, § 2).

[12] *Worth* v. *Seldin,* 422 U.S. 490, 498 (1975); *Focus on the Family* v. *Pinellas Suncoast Transit Auth.,* 344 F.3d 1263, 1275 (11th Cir. 2003).

[13] *Lujan* v. *Defenders of Wildlife,* 504 U.S. 555, 560 (1992).

[14] *Id.*

[15] *Id.*

[16] *Id.* at 560-61.

[17] 133 S. Ct. 1138 (2013).

[18] *See, e.g., Irwin* v. *RBS Worldpay, Inc.,* 1:09-CV-0033-CAP, 2010 U.S. Dist. LEXIS 145301, at *13-15 (N.D. Ga.2010).

[19] *See, e.g., Willingham* v. *Global Payments, Inc.,* L12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *20 (N.D. Ga. 2013).

[20] *See, e.g, Reilly* v. *Ceridian Corp.,* 664 F.3d 38, 46 (3d Cir. 2011).

[21] *Krottner v. Starbucks Corp.,* 628 F.3d 1139, 1143 (9th Cir. 2010); *Pisciotta* v. *Old Nat'l Bancorp,* 499 F.3d 629, 634 (7th Cir. 2007).

[22] *Krottner,* 628 F.3d at 1143.

[23] *Id.*

[24] 50 U.S.C. § 1881a.

[25] *Clapper,* 133 S. Ct. at 1142.

[26] *Id.* at 1140.

[27] *Id.* at 1143.

[28] *Id.*

[29] *Id.* at 1147.

[30] *Id.* at 1150.

[31] *Id.*

[32] *Id.* at 1151.

[33] 27 F. Supp. 3d 871, 876 (N.D. 111. 2014).

[34] *Id.*

[35] *Id.*

[36] 4:14-CV-2872, 2015 U.S. Dist. LEXIS 16451, at *14 (S.D. Tex. February 11, 2015).

[37] *Id.*

[38] *Id.*

[39] *See, e.g., In re Sony Gaming Network & Customer Data Sec. Breach Litig, 996* F. Supp. 2d 942, 961-62 (S.D. Cal. 2014); *Moyer v. Michaels Stores, Inc.,* 14-C-561, 2014 U.S. Dist. LEXIS 96588, at *13-19 (N.D. 111. 2014).

[40] 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126 (N.D. Cal. 2014).

[41] *Adobe,* 2014 U.S. Dist. LEXIS 124126, at *28.

[42] *Id.*

[43] *Id.*

[44] 28 U.S.C. § 1331.

[45] 28 U.S.C. § 1332(d)(2). *See, e.g., Corona v. Sony Pictures Entm't, Inc.,* 2:14-CV-09600-RGK-SH (C.D. Cal. filed Dec. 15, 2014).

[46] *See, e.g., Manlove* v. *Unified Gov't of Athens,* 285 Ga. 637, 638 (2009).

[47] 301 Ga. App. 569, 572 (2009), *overruled on other grounds by Cumberland Contractors, Inc. v. State Bank & Trust Co.,* 327 Ga. App. 121, 126 (2014).

[48] *Id.*

[49] *Id.* (citing *Dry Storage Corp.* v. *Piscopo,* 249 Ga. App. 898, 900 (2001)).

[50] *Id.* (citing *Killian* v. *Green Tree Servicing, LLC (In re Killian),* 05-14629-HB, 2009 Bankr. LEXIS 2030, at *27-29 (Bankr. D.S.C. 2009)).

[51] 315 Ga. App. 573,576(2012).

[52] *Id.* at 576-77.

[53] *Johnson* v. *Am. Nat'l Red Cross,* 276 Ga. 270 (2003).

[54] *Id.* at 275.

[55] *Boyd v. Orkin Exterminating Co., Inc.,* 381 S.E.2d 295, 298 (1989), *overruled on other grounds by Hanna* v.*McWilliams,* 213 Ga. App. 648 (1994).

[56] *Id.*