Corporate Litigation:

Standing to Bring Consumer Data Breach Claims

Joseph M. McLaughlin*
Simpson Thacher & Bartlett LLP

April 14, 2015

Security experts say that there are two types of companies in the United States: "those that have been hacked and those that don't know they've been hacked."[1] More and more companies have been experiencing data breaches, and "the absolute size of the breaches is increasing exponentially."[2] Predictably, consumers who believe their personal and/or financial information was compromised by a data breach have been suing the breached companies. But there is a threshold question with which courts have been grappling in recent data breach cases: Have the consumer plaintiffs suffered an actual harm sufficient to establish standing to sue in federal court under Article III of the Constitution?

Last month, a Minnesota federal judge preliminarily approved a class action settlement between Target Corporation and a class of consumers asserting claims arising from the 2013 breach of Target's computer network, which affected the personal and/or financial information of up to 110 million customers. Target agreed to pay a total of $10 million to consumers "whose credit or debit card information and/or whose personal information was compromised as a result of the data breach" and to implement and maintain specified data security measures for a period of five years.[3]

The Minnesota district court had denied Target's motion to dismiss in December 2014, permitting the majority of the plaintiffs' claims to move forward, and ruling that the plaintiffs had standing to pursue their claims against the retailer. The standing ruling departed from many other recent consumer data breach case rulings, in which courts—often relying on the Supreme Court's 2013 Article III standing decision in *Clapper v. Amnesty International USA*—have determined that consumer plaintiffs did not adequately allege actual injury. The decision in *In re Target Corporation Consumer Data Security Breach Litigation* may be unsettling for corporations, as it suggests that, at least in certain jurisdictions, consumer data breach actions may be a more serious threat than previously thought.

Clapper Decision

In *Clapper*, the Supreme Court reiterated that under Article III, plaintiffs must establish standing to sue by demonstrating an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[4] Equally importantly, the opinion clarified that "threatened injury must be certainly impending to constitute injury in fact,' and that '[a]llegations of possible future injury' are not sufficient."

Clapper addressed whether the respondents had standing to assert a constitutional challenge to Section 702 of the Foreign Intelligence Surveillance Act, which authorizes the Attorney General and the Director of National Intelligence, after obtaining the approval of the Foreign Intelligence Surveillance Court, "to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States." The respondents were "attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to

* ***Joseph M. McLaughlin*** *is a partner at Simpson Thacher & Bartlett LLP. Yafit Cohn, an associate at the firm, assisted in the preparation of this article.*

engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad" whom respondents believed to be likely targets of surveillance.

Seeking a declaration that Section 702 is unconstitutional and a permanent injunction against authorized surveillance under the provision, the respondents advanced two theories of standing. First, the respondents claimed that "they can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under [Section 702] at some point in the future." Second, the respondents asserted that they were suffering present injury, because the substantial risk of surveillance under Section 702 has already impelled them "to take costly and burdensome measures to protect the confidentiality of their international communications."

Addressing the respondents' first argument, the court held that an assertion that there is "an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted" pursuant to Section 702 at some future time "relies on a highly attenuated chain of possibilities," and thus "does not satisfy the requirement that threatened injury must be certainly impending." The court similarly rejected the respondents' alternative argument—namely, that they have standing by virtue of the various "costly and burdensome measures" they have allegedly taken to protect the confidentiality of their communications with their foreign contacts. The court stated that because the harm respondents sought to avoid was "not certainly impending," a theory of standing based on a reaction to the risk of such harm is "unavailing."

Application of 'Clapper'

Post-*Clapper*, corporate defendants in data breach actions argued—with considerable success—that the standard announced in *Clapper* precludes consumer plaintiffs from asserting "actual and imminent injury" under Article III. *In re Barnes & Noble Pin Pad Litigation*[5] is illustrative. An Illinois federal court ruled that the consumer plaintiffs in a putative data breach class action lacked standing to bring an action against Barnes & Noble, which had publicly announced a security breach that may have compromised customers' credit and debit card information. According to the plaintiffs, Barnes & Noble "did not adhere to security protocols and regulations mandated by its credit partners, such as Visa and other members of the payment card industry" and when the breach did occur, delayed public announcement of the breach by six weeks and never directly notified customers of the breach.

The plaintiffs had argued that as a result of the breach, they suffered various damages, including, among others, "untimely and inadequate notification of the security breach, improper disclosure of their personal identifying information or 'PII', loss of privacy, expenses incurred in efforts to mitigate the increased risk of identity theft or fraud, time lost mitigating the increased risk of identity theft or fraud, [and] an increased risk of identity theft."

In addition to finding that improper disclosure of PII and loss of privacy were insufficient to establish standing because the plaintiffs failed to allege facts to support that their information was disclosed, the court rejected the plaintiffs' claim that the defendant's untimely and/or inadequate notification of the breach increased the risk that the plaintiffs will suffer "some actual injury" as a result of the breach. Citing *Clapper*, the court explained that "[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing"; according to the court, the complaint did not indicate that the plaintiffs "have suffered either a 'certainly impending' injury or a 'substantial risk' of an injury, and therefore, the increased risk is insufficient to establish standing."

Rejecting the claims of increased risk of identity theft and time and expenses incurred to mitigate the risk of identity theft, the court relied on *Clapper*, holding that "speculation of future harm does not constitute actual injury." The court stated that the "only cognizable potential injury alleged" in the complaint was a fraudulent charge on one plaintiff's credit card following the breach, but the court held that not only was it unclear that this charge resulted from Barnes and Nobles' security breach, but the plaintiff did not plead "that actual injury resulted and that she suffered any monetary loss due to the fraudulent charge." The court opined that "[i]n order to have suffered an actual injury, she must have had an unreimbursed charge on her credit card."

Other courts have reached similar conclusions, often in reliance on *Clapper*. In *Peters v. St. Joseph Services Corp.*,[6] for example, the Texas district court dismissed the consumer's complaint on the grounds that the purported increased risk of identity theft/fraud was "speculative" and thus did not constitute "certainly impending" injury and that the plaintiff "has not alleged any quantifiable damage or loss she has suffered as a result of the Data Breach." Likewise, in *Storm v. Paytime*, a Pennsylvania district court held that a heightened risk of identity theft "does not suffice to allege an imminent injury" and that, as the Clapper court warned, damages in the form of plaintiffs' increased expenses related to measures they took to prevent themselves from identity theft following the breach may not be used to "manufacture" standing.[7]

The Target Decision

The Target decision diverges from the majority of post-*Clapper* data breach cases, but is not the first instance of a court recognizing Article III standing in a consumer data breach action.[8] However, the Target court's decision to allow customers in "one of the largest data breaches of payment-card security in United States retail history" to proceed with their lawsuit introduces a higher level of uncertainty over whether corporate defendants in a data breach action will be able to prevail on a motion to dismiss on standing grounds.[9]

In *Target*, a putative class of consumers whose account and/or personal identifying information was allegedly stolen as a result of the Target data breach brought statutory and common law claims against the retailer, claiming that "Target's conduct—failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' financial account and personal data, and failing to provide timely and adequate notice of the Target data breach"—caused them substantial harm.[10] Specifically, the plaintiffs asserted manifold injuries, including:

- Unauthorized charges on their debit/credit card accounts;
- Theft of personal and financial information;
- Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- Injury "flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of" their information on the internet's black market for debit/credit cards;
- "[D]amages to and diminution in value of their personal and financial information entrusted to Target" with the "mutual understanding that Target would safeguard" their data;
- "[M]oney paid for products purchased at Target stores," since the plaintiffs "would not have shopped at Target had Target disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Target provided timely and accurate notice of the Target data breach."

Addressing Target's motion to dismiss, Minnesota federal district Judge Paul A. Magnuson first addressed Target's "primary argument"—that "Plaintiffs do not have standing to raise any of their claims because Plaintiffs cannot establish injury." Like successful corporate defendants in many previous data breach actions, Target contended that "Plaintiffs' claimed injuries are not actual or imminent." But Judge Magnuson rejected this argument (interestingly, without reference to *Clapper*), noting that the complaint recites "many of the individual named Plaintiffs' injuries, including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees." The court also credited the plaintiffs' allegation that "had Target notified its customers about the data breach in a timely manner," they "could not have shopped at Target."

The court rejected the notion that "because some Plaintiffs do not allege that their expenses were unreimbursed or say whether they or their bank closed their accounts, Plaintiffs have insufficiently alleged injury." The court thus held that the plaintiffs' allegations were sufficient at the motion to dismiss stage to plead standing. The court observed, however, that "[s]hould discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment" on the standing issue.

Significance of Decision

Judge Magnuson did not address all of the plaintiffs' alleged injuries, leaving undecided whether some of them—standing alone—would suffice as actual injury. Most notably, Judge Magnuson did not specifically discuss the alleged heightened risk of identity theft or plaintiffs' alleged increased expenses to protect themselves from the risk of identity theft, which some previous decisions have found to be insufficient to plead standing. However, Judge Magnuson's opinion clarifies that at least in some jurisdictions, plaintiffs in data breach actions can establish standing by plausibly pleading economic injury in the form of unreimbursed fees, even without unreimbursed, fraudulent charges on their credit cards post-breach. Additionally, Judge Magnuson's opinion recognizes that, at least when pleading violations of state data breach notice statutes and unjust enrichment, plaintiffs may have standing if they plead that they "would not have shopped" at the retailer if they had been adequately notified of the breach in a timely fashion.

It is unknown whether other courts will follow Judge Magnuson's ruling, but the decision suggests how plaintiffs may be able to craft their complaints to try to circumvent *Clapper* and serves to caution corporate defendants that in certain jurisdictions—depending on the particular facts and circumstances alleged—a putative consumer class action arising from a data breach may not be so simple to dispose of on a motion to dismiss. It would not be surprising if the Target decision spurs additional data breach litigation, encouraging more consumer plaintiffs to allege those injuries that Judge Magnuson recognized as sufficient, at least at the pleading stage.

Endnotes:

1. Nicole Perlroth, "The Year in Hacking, by the Numbers," N.Y. Times, April 22, 2013.

2. *Storm v. Paytime*, 2015 WL 1119724 (M.D. Pa. Mar. 13, 2015) (citing Elizabeth Weise, "43% of Companies Had a Data Breach in the Past Year," USA TODAY, Sept. 24, 2014).

3. Order Certifying A Settlement Class, Preliminarily Approving Class Action Settlement and Directing Notice to the Settlement Class at 2, *In re Target Corp. Consumer Data Security Breach Litig.*, MDL No. 14-2522 (D. Minn. March 19, 2015) (Dkt. 364). The settlement agreement does not affect the putative class action litigation, currently pending in the District of Minnesota, which was brought against Target by financial institutions that issue debit and credit cards claiming to have been injured as a result of the breach.

4. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (citing *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752 (2010)).

5. *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

6. 2015 WL 589561 (S.D. Tex. Feb. 11, 2015).

7. 2015 WL 1119724, at *6-*7.

8. See, e.g., *In re Sony Gaming Networks & Customer Data Sec. Breach Litig*., 996 F.Supp.2d 942, 962 (S.D. Cal. 2014) (finding that "Plaintiffs have plausibly alleged a 'credible threat' of impending harm based on the disclosure of their Personal Information following the intrusion"); *Moyer v. Michaels Stores*, 2014 WL 3511500, at *6 (N.D. Ill. Jul. 14, 2014) (concluding that "elevated risk of identity theft stemming from the data breach…is sufficiently imminent to give Plaintiffs standing"); *In re Zappos.com*, 2013 WL 4830497, at *2 (D. Nev. Sept. 9, 2013) (holding that plaintiffs have standing because they sufficiently alleged that "they have had to pay money to monitor their credit scores and secure their financial information due to the increased risk of criminal fraud against them occasioned by Defendant's negligent loss of their personal information").

9. *In re Target Corp. Customer Data Security Breach Litig*., 2014 WL 7192478, at *1 (D. Minn. Dec. 18, 2014).

10. Consumer Plaintiffs' First Amended Consolidated Class Action Complaint at 1, *In re Target Corp. Consumer Data Security Breach Litig*., MDL No. 14-2522 (D. Minn. Dec. 1, 2014) (Dkt. 258).
