Hackers stole your clients' information. Here are practical tips to help them recover for their injuries in this emerging area of consumer class actions.

By || **Norman Siegel, Barrett Vahle, and J. Austin Moore**

SECURING DATA-BREACH CLAIMS

In the past year alone, many high-profile companies—including retailers, restaurants, health care companies, and financial institutions—fell victim to well-publicized breaches of electronic data. This unfortunate trend shows no signs of slowing down. The drastic increase in cyberattacks has created an emerging area of class action litigation over lax cybersecurity practices and consumer-related data-breach claims.

These cases typically involve a similar set of facts: An unauthorized third party hacks into a company's computer servers to steal customer information. This information may include customers' names, addresses, Social Security numbers, and personal financial information such as credit and debit card numbers, card expiration dates, and cardholder verification values. The hackers then sell this information in bulk on the black market. Often, the company does not learn of the breach until thousands of customers experience fraud or unauthorized charges.

In many cases, the breach was possible only because the company ignored warning signs or failed to take reasonable steps to protect customer information. For example, the company may have failed to secure its servers properly, implemented outdated security software, or knowingly understaffed its information technology department. The company may also be liable for not notifying customers of a breach in a timely manner.

Standing to Sue

In considering whether to file a data-breach class action, the first and most important question to consider is what injuries

your clients suffered and whether those are sufficient to confer standing. In the data-breach context, standing is almost always the subject of a motion to dismiss.

Few would dispute that customers who experienced unreimbursed, unauthorized charges on their accounts suffered a cognizable injury sufficient to confer standing. But what about customers who were reimbursed by their bank for the unauthorized charges? Or those who spent time and effort obtaining replacement cards or lost temporary access to their funds because their accounts were frozen? What about customers who preemptively purchased credit monitoring services to minimize future risk? Courts routinely grapple with questions such as these when considering standing in these cases.

The standing analysis begins with the seminal Supreme Court decision *Clapper v. Amnesty International USA*.[1] In that case, various organizations argued that a provision of the Foreign Intelligence Surveillance Act allowing surveillance of certain people was unconstitutional. The Court held that the plaintiffs lacked standing because they did not present evidence that their communications were actually monitored and because it was "highly speculative" whether their communications would be targeted imminently.[2] The Court reiterated that, to establish standing, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[3] The threatened injury also must be "certainly impending," and "allegations of possible future injury" are not sufficient to confer standing.[4]

While the facts of *Clapper* have little in common with the typical data-breach scenario, defense attorneys have successfully used the ruling to argue that plaintiffs who have had personal information stolen lack standing because there is no "certainly impending" injury.[5] The "increased risk" of future harm—typically unauthorized charges or identity theft—is too speculative, they say.

You can counter these arguments in several ways under *Clapper*.

Allege injuries in detail. When plaintiffs have not yet experienced fraud or unauthorized charges, it is important to allege in detail other injuries and hardships they experienced because of the data breach. Common, real-life consequences of a data breach include

- spending significant time and expense searching for fraudulent charges
- canceling and reissuing credit and debit cards
- purchasing credit monitoring and identity theft prevention
- having withdrawal and purchasing limits imposed on compromised accounts
- being unable to withdraw funds from compromised accounts
- resetting automatic billing instructions tied to compromised accounts
- paying late fees and declined-payment fees from failed automatic payments.

The more detail you include, the better. For example, if a plaintiff loses account access for several days while waiting for a replacement card and has to borrow money or cannot pay rent on time, the court may be persuaded that anyone who lost access to funds had the potential to suffer a similar injury. Because *Clapper* requires that the injury be actual *or* imminent, any of the real-life consequences above *could* constitute injuries, even if unauthorized charges have not yet manifested.

Because individualized damages can potentially cause problems when seeking class certification, consider engaging an expert who can prepare a damages model demonstrating that damages incurred by the putative class can be calculated on a classwide basis. Alternatively, you can seek certification under Rule 23(c)(4), which allows a court to evaluate key liability issues that affect the entire class while leaving individualized damages proof for another day. In other cases, where the primary relief sought is injunctive, consider seeking certification under Rule 23(b)(2), which eliminates potential vulnerabilities in certifying a class with varying damages.

> IN MANY CASES, THE BREACH WAS POSSIBLE ONLY BECAUSE THE COMPANY IGNORED WARNING SIGNS OR FAILED TO TAKE REASONABLE STEPS TO PROTECT CUSTOMER INFORMATION.

Named plaintiffs should represent different injuries. In a class action, named plaintiffs representing a class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent."[6] Therefore, the named plaintiffs' injuries should be representative of different injuries in the case. Structuring the case this way presents the court with a spectrum of injuries that it may

not have previously considered. From a practical standpoint, having each named plaintiff represent a different category of injury makes it easier for the court to apply a standing analysis to each—even if the court ultimately allows only certain plaintiffs to maintain their cases. This structure makes it more difficult for a court to dismiss the entire case, especially when at least one plaintiff represents individuals who suffered unreimbursed, unauthorized charges.

If you are pursuing a multi-state complaint that includes state-specific causes of action, it is preferable to name plaintiffs who are residents of each state seeking to be represented or risk having claims under the laws of those jurisdictions dismissed for lack of standing.

Use* Clapper *to your advantage. Instead of downplaying *Clapper*, use it to make a compelling case for standing. Although defendants often argue that the *Clapper* Court intended to raise the bar for standing by using the phrase "certainly impending," lower courts have been reluctant to agree.[7] For example, in *In re Adobe Systems, Inc., Privacy Litigation*, the district court judge noted that "*Clapper* did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability."[8] The decision was not intended to change "well-established standing principles" but rather to caution courts from "accepting a too-speculative theory of future injury."[9]

In *Clapper*, the Supreme Court observed that conferring standing in that case required five hypothetical steps and "guesswork as to how independent decisionmakers will exercise their judgment."[10] Because the plaintiffs presented no evidence that their specific communications were monitored or were likely to be monitored in the future, a "highly attenuated chain of possibilities" did not result in a "certainly impending" injury.[11]

In data-breach cases, by contrast, hackers steal customers' personal and financial information with one goal in mind: to sell it on the black market. Often, the potential harm has already surfaced for many similarly situated individuals. It is also common for hackers to sell batches of cardholder information in waves—months or years apart—to avoid immediate detection. As the court noted in *Adobe*, when "stolen data has already surfaced on the Internet . . . the danger that plaintiffs' stolen data will be subject to misuse can plausibly be described as 'certainly impending.' "[12] "[T]o require plaintiffs to wait until they actually suffer identity theft or credit card fraud 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."[13]

In further contrast to *Clapper*, where the plaintiffs could not show that their information had been or would be monitored, companies subject to data breaches can typically confirm whether customer information was compromised.

Plaintiffs can raise these points not only to distinguish the facts of the *Clapper* case, but also to highlight their own damages and more immediate risk of future harm.

Causes of Action

After jumping over the standing hurdle, you must determine which causes of action to present. Consider the following claims.

Violations of state consumer protection statutes. Every state has laws to protect its citizens from fraud, misrepresentation, or unfair or deceptive practices. These vary from state to state—and data-breach claims do not always fit comfortably within them—but some theories have gained traction with courts.

For example, in *Target Corp. Customer Data Security Breach Litigation*,[14] the federal district court considered four theories of consumer protection violations under the laws of 49 states and the District of Columbia. The plaintiffs claimed Target violated state consumer protection laws by

- failing to maintain adequate computer systems and data security practices.
- failing to disclose these inadequate computer systems.
- failing to properly notify customers of the data breach.
- continuing to accept credit and debit card payments after it should have known of the data breach and before it purged the malware.[15]

Target argued that the plaintiffs did not sufficiently plead economic injury. The court disagreed, holding that "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees" constitute an injury.[16] It reiterated this point regarding consumer protection claims: "Plaintiffs have pled economic injury, in the form of unreimbursed late fees, new card fees, and other charges," and "ascertainable loss" as required under some state statutes "is in general not limited to only purely economic loss."[17] This highlights the

MORE ON DATA BREACH CLAIMS

Visit the Web pages below for additional information.

AAJ SECTION
Business Torts
www.justice.org/sections

AAJ LITIGATION GROUP
Consumer Privacy/Data Breach
www.justice.org/litgroups

AAJ EDUCATION PROGRAM
2014 Annual Convention: Business Torts Section CLE Program
www.playbackaaj.com

AAJ PRESS
Litigating Tort Cases, Roxanne Conlin and Gregory Cusimano, Eds.
www.justice.org/aajpress

PROVING INJURY CAN BE COMPLICATED IN STATES THAT RECOGNIZE THE CONFUSING AND OFTEN MISAPPLIED ECONOMIC LOSS DOCTRINE.

importance of having a diverse group of named plaintiffs with articulable injuries.

The *Target* court dismissed claims from states whose statutes explicitly prohibit private rights of action[18] or class actions.[19] Other state-specific issues to consider are whether the claims require reliance on the misrepresentation or omission (creates issues for class certification), whether omissions are actionable only if the defendant has a duty to disclose, and whether the remedy is limited to only injunctive relief.

Violations of state data-breach notification statutes. Most states have data-breach notification laws. Common threads are who must abide by the law, what constitutes a breach of "personal information," and the requirements for timely notification. These claims allege the defendant failed to timely notify customers of the breach.

While these statutes are promising, most do not expressly provide for a private right of action,[20] have not been tested yet in court, and do not provide for statutory damages or attorney fees. So recovery typically is limited to injunctive relief or actual losses.

In *Target*, the court undertook likely the most comprehensive analysis to date of statutory data-breach notification claims. It dismissed claims under the laws of Arkansas, Connecticut, Idaho, Massachusetts, Minnesota, Nebraska, Nevada, and Texas because they limited enforcement to the state's attorney general,[21] but it allowed claims under the 26 state laws that used "ambiguous language or non-exclusive remedies"[22] or were silent on the issue of who may enforce the law.[23]

Negligence. Common law negligence claims remain viable in most of these cases, based on allegations of duty, breach, causation, and injury. If the plaintiffs can allege the defendant owed a duty to protect customers' personal information, the first three elements are relatively uncontroversial.

The injury requirement, however, has proved more challenging. Even courts that have found sufficient injury to confer Article III standing have dismissed negligence claims because the plaintiffs cannot show pecuniary loss.[24] Proving injury can be even more complicated in states that recognize the confusing and often misapplied economic loss doctrine, in which a plaintiff can recover economic damages only if also claiming some form of physical harm (such as personal injury or property damage). Thus, in actions for negligence, liability in states recognizing the doctrine is limited to damages for physical injuries, and recovery of economic loss is not allowed.[25]

The rationale behind the economic loss doctrine is that tort law provides the proper remedy for personal injury or property damage, while contract law and the Uniform Commercial Code provide the proper remedy "for economic loss stemming from diminished commercial expectations."[26] While this rationale does not fit most data-breach cases because the parties have not necessarily allocated risk through contract, many courts are tied to (often inconsistent) precedent barring such claims.[27] Still, most states recognize exceptions that may apply in data-breach cases. For example, if an "independent duty" exists outside contractual obligations, the economic loss doctrine does not bar a tort claim in some states.[28] Likewise, the doctrine does not apply where there is a "special relationship" between the parties.[29]

In *Target*, the court considered the economic loss rule under the laws of 11 states and ultimately barred claims in Alaska, California, Illinois, Iowa, and Massachusetts because courts in those states had decisions on point barring similar claims. The *Target* court permitted negligence claims to proceed in states that did not recognize the rule, and it applied relevant exceptions where no state-specific law barred application.[30]

Breach of implied contract. Depending on the details of the parties' relationship, another potentially viable cause of action is breach of an implied contract to safeguard plaintiffs' personal and financial information. The First Circuit explained its rationale for applying implied contract principles to data-breach cases:

> When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect—and certainly does not intend—the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract.[31]

The courts in *In re Michaels Stores Pin Pad Litigation* and *Target* adopted this rationale and rejected motions to dismiss claims for breach of implied contract.[32]

Unjust enrichment. Unjust enrichment is premised on the theory that a party who has been unjustly enriched at the expense of another should be

required to make restitution.

When the data-breach defendant is a retailer, this claim is typically that the defendant was unjustly enriched because the plaintiffs were "overcharged" for goods or services because some portion of the purchase price was meant to be used for adequate security, or that the plaintiffs simply would not have purchased items from the defendant had they known about the lack of adequate security.

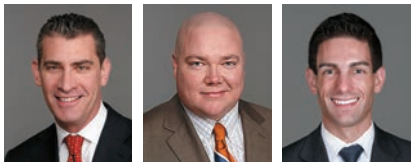
Courts have found little merit to the "overcharge" theory because it is rarely accompanied by allegations that the retailer "charged a higher price for goods [when] a customer pays with credit, and therefore, that additional value is expected in the use of a credit card."[33]

But the second theory has gained more traction. In *Target*, the court observed that the "would not have shopped" theory is plausible because if

> plaintiffs can establish that they shopped at Target after Target knew or should have known of the breach, and that plaintiffs would not have shopped at Target had they known about the breach, a reasonable jury could conclude that the money plaintiffs spent at Target is money to which Target "in equity and good conscience" should not have received.[34]

Other common law property torts, such as bailment, have not fared well with courts.[35]

While courts have not yet tested many legal theories in this emerging area of law, the above causes of action are a good place to start when pursuing a data-breach class action. As data breaches have become more commonplace, courts have been increasingly willing to recognize standing and new theories of injuries related to the theft of personal information. Even so, expect an array of twists and turns as courts engage in this emerging area of litigation.



Norman Siegel *and* **Barrett Vahle** *are partners with Stueve Siegel Hanson in Kansas City, Mo., and* **J. Austin Moore** *is an associate with the firm. They can be reached at siegel@stuevesiegel.com, vahle@stuevesiegel.com, and moore@stuevesiegel.com. The authors are currently serving in leadership roles in consumer multidistrict litigation against Target and the Home Depot.*

Notes

1. 133 S. Ct. 1138 (2013).
2. *Id.* at 1148.
3. *Id.* at 1147 (internal quotation and citation omitted).
4. *Id.*
5. *See e.g. Remijas v. Neiman Marcus Group, LLC*, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014); *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014).
6. *Warth v. Seldin*, 422 U.S. 490, 502 (1975).
7. *See e.g. In re Sony Gaming Networks & Customer Data Sec. Breach Litig.* ("*Sony II*"), 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014) ("*Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.' ").
8. 2014 WL 4379916 at *7 (N.D. Cal. Sept. 4, 2014).
9. *Id.*
10. 133 S. Ct. at 1150. In *Clapper*, the "too-speculative" chain of events that had to take place for plaintiffs to have standing to sue included: "(1) the government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the government will choose to invoke its authority under [the FISA section at issue] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the [FISA] court will conclude that the government's proposed surveillance procedures satisfy [FISA's] many safeguards and are consistent with the Fourth Amendment; (4) the government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the government intercepts." *Id.* at 1148.
11. *Id.* at 1148.
12. *In re Adobe Sys., Inc. Priv. Litig.*, 2014 WL 4379916 at *8.
13. *Id.*
14. 2014 WL 7192478 (D. Minn. Dec. 18, 2014).
15. *Id.* at *5.
16. *Id.* at *2.
17. *Id.* at *5.
18. Delaware and Oklahoma.
19. Alabama, Georgia, Kentucky, Louisiana, Mississippi, Montana, South Carolina, and Tennessee. An additional two states, Ohio and Utah, allow class pursuit of consumer-protection claims only if the challenged act has been declared deceptive by a final court judgment or by the state's attorney general.
20. You can argue in some states that, even without a private right of action, the data-breach statute can be enforced through the state's consumer-protection statute. *See Target*, 2014 WL 7192478 at *10.
21. *Id.* at **11–12.
22. *Id.* at **12–13 (including Colorado, Delaware, Iowa, Kansas, Michigan, and Wyoming).
23. *Id.* at **13–14 (including Georgia, Kentucky, and Wisconsin). Yet the court construed the Rhode Island statute's silence on enforcement as prohibiting private rights of action. *Id.*
24. *See e.g. In re Sony Gaming Networks & Customer Data Sec. Breach Litig.* ("*Sony I*"), 903 F. Supp. 2d 942, 960–61 (S.D. Cal. 2012); *see also Krottner v. Starbucks Corp.*, 406 Fed. Appx. 129, 131 (9th Cir. 2010).
25. *Sony I*, 903 F. Supp. 2d at 960–61.
26. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528–29 (N.D. Ill. 2011).
27. *See e.g. id.* at 528; *see also Sony II*, 996 F. Supp. 2d at 967–68.
28. *See Target*, 2014 WL 7192478 at **15–20.
29. *Id.* A "special relationship" may exist where the plaintiff is an intended beneficiary of the defendant's obligations under a contract, the plaintiff's loss was foreseeable, the plaintiff was highly likely to suffer the loss from the defendant's conduct, the defendant's conduct is closely connected to the plaintiff's loss, the defendant's conduct is morally blameworthy, and the public policy favors holding the defendant responsible for the plaintiff's economic loss. *J'Aire v. Gregory*, 24 Cal. 3d 799, 804 (1979); *Biakanja v. Irvine*, 320 P.2d 16, 19 (Cal. 1958).
30. *Target*, 2014 WL 7192478 at **15–20.
31. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011).
32. 830 F. Supp. 2d at 531–32; 2014 WL 7192478 at **20–21.
33. *Barnes & Noble*, 2013 WL 4759588 at *5; *see also Target*, 2014 WL 7192478 at **22–23.
34. 2014 WL 7192478 at *23.
35. *See Sony I*, 903 F. Supp. 2d at 974–75; *Target*, 2014 WL 7192478 at *21.