dri
The Voice of the Defense Bar




Riding the E&O Line

The Newsletter of the Professional Liability Committee

3/28/2014 **Volume 6 Issue 1**

In this Issue

Hacked: How Target's Data Breach Affects the Cyber Liability Landscape

by Thomas Hutchinson and Nels Vulin

December's news of Target Corp.'s massive security breach—cyber attackers took names, phone numbers, and email addresses of an estimated 70 million customers—has resulted in a flood of litigation. The retail giant now faces scores of lawsuits, with more expected to come. As companies improve their security systems to protect customer information in the wake of one of the largest cyber-attacks ever, lawyers and carriers will need to keep an eye on the Target lawsuits, the outcome of which could affect who may be held liable when data is compromised and what damages may be recovered.

Two main groups have brought lawsuits against Target, and more could follow. Already, customers and banks have filed actions against the retailer. *See Purcell v. Target Corp*., No., 3:13-cv-02274-JE (D. Or. filed Dec. 20, 2013) (customer action); *Putnam Bank v. Target Corp*., No. 0:14-cv-00121-DSD-JSM, (D. Minn. filed Jan. 13, 2014) (bank action). State attorneys general may also sue the company for violating customer protection statutes, though none have done so yet. And, depending on the developing facts, Target's shareholders may bring claims against the company for failing to disclose security vulnerabilities. But Target is not likely to be the only defendant. In addition to

Join a Committee

Committee Leadership

Committee Chair
Frances M. O'Meara
Thompson Coe & O'Meara

the merchant itself, third parties—such as vendors—could face liability for their roles in the attack. No matter the parties, however, lawsuits connected to the security lapse are likely to face substantial challenges, which could draw out litigation for years to come.

Target's customers have already brought suit. The causes of action alleged by these plaintiffs vary, but claims of negligence and violation of statutory notification requirements are common to nearly all of the actions. With regard to negligence, most plaintiffs allege that that Target failed to (1) maintain security systems sufficient to protect consumer information; (2) comply with industry standards for cyber protection; and (3) promptly notify customers that the information was leaked. *See Purcell v. Target Corp*., No., 3:13-cv-02274-JE (D. Or. filed Dec. 20, 2013) (asserting a class action with claims of negligence and violation of Oregon's Unlawful Trade Practices Act.)

As some legal commentators have noted, to demonstrate Target's liability for any cause of action, many customers will first need to cross the standing threshold. As Reuters' Alison Frankel points out, this could be tricky given that courts have been far from uniform in establishing standards for standing to bring claims related to data security breaches. Alison Frankel, *Why (Most) Consumer Data Breach Class Actions vs Target Are Doomed*, Reuters, Jan. 13, 2014, http:// http://blogs.reuters.com/alison-frankel/2014/01/13/why-most-consumer-data-breach-class-actions-vs-target-are-doomed/. The controlling case is arguably the U.S. Supreme Court's decision in *Clapper v. Amnesty International*, 568 U.S. ___ (2013), which requires plaintiffs to show actual harm or, at the very least, that harm is "certainly impending." Because fear that an injury could or might occur is not enough under *Clapper*, Target can argue that most customers do not have standing to bring claims based only on the mere possibility that personal information was misused. As Frankel points out, courts have already relied on *Clapper* as grounds to dismiss cyber breach class actions, including claims against Barnes & Noble, *In re. Barnes & Noble Pin Pad Litigation*, No. 1:12-cv-08617 (N.D. Ill., E. Div., filed Sept. 3, 2013); and an action claiming warehouse retailer Sam's Club deceived customers about its cyber security, *Hammer v. Sam's East, Inc.*, No. 12-cv-2618-CM, 2013 WL 3756573 (D. Kan. July 16, 2013).

Of course, this is far from a well-settled area of law, and Target customers may be able to convince a court that they have standing despite *Clapper*. In one of the most heavily-litigated cyber security lawsuits in recent years, Sony failed to convince the court that the class action plaintiffs lacked standing because their alleged harm was not actual or immediate. *In re Sony Gaming Networks &*

Thompson Coe & O'Meara
fomeara@thompsoncoe.com

Vice Chair
David L. Brandon
Morris Polich & Purdy
dbrandon@mpplaw.com

Publications Chair
Marissa I. Delinks
Hinshaw & Culbertson LLP
mdelinks@hinshawlaw.com

Click to view entire Leadership

Upcoming Seminar

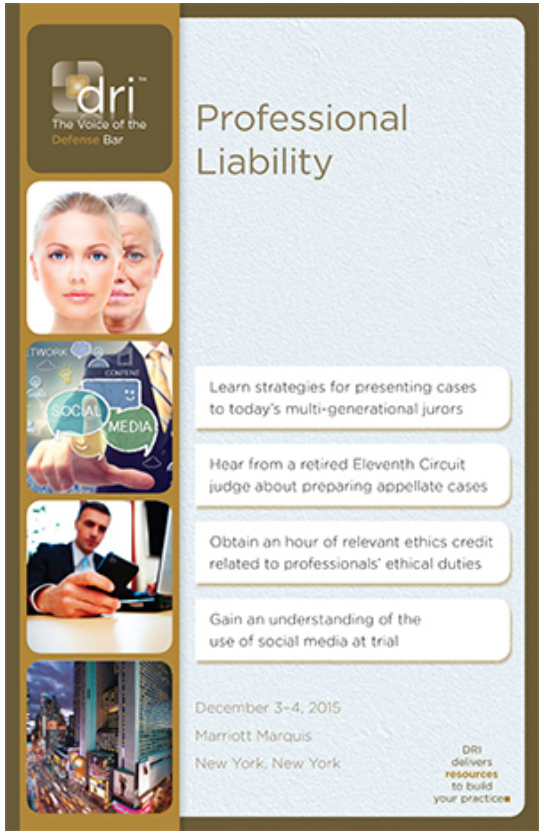
Customer Data Sec. Breach Litig., MDL 11MD2258 AJB MDD, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014).The *Sony* court denied the defendant's motion to dismiss on those grounds, finding that *Clapper* was not fatal to the plaintiffs' claims. *Id.* at *9.. This ruling may provide some support for the Target plaintiffs' argument that even though they may not have lost a dime thus far, they still have been harmed by the attack.

Customers are not the only potential plaintiffs in actions against Target. Several banks have also sued to recover expenses incurred as a result of the breach, including the costs of reimbursement of fraudulent charges, closing customer accounts, and issuing new credit and debit cards to customers. One such lawsuit, filed by Connecticut-headquartered Putnam Bank in January, is typical of actions that have been brought by banks. *Putnam Bank v. Target Corp.*, No. 0:14-cv-00121-DSD-JSM ((D. Minn. filed Jan. 13, 2014). In that lawsuit Putnam alleges claims of negligence, negligent misrepresentation, breach of contract, and violations of several state and federal statutes, including Minnesota's unfair and deceptive trade practices statute, the federal Gramm-Leach-Bliley Act's deceptive acts prohibitions, and Minnesota's consumer notification statute.

Like the consumer actions, Putnam's lawsuit—which has been stayed pending a decision on transfer and consolidation—claims that Target failed to implement reasonable security measures that met industry standards. Damages, Putnam alleges, include the costs of reimbursing customers and associated administrative expenses. Based on the *Putnam* case, it seems that banks, compared to customers, may have an easier time demonstrating harm, given their fairly direct and quantifiable injuries.

If history is any indication, however, the banks' lawsuits are likely to settle long before trial. In the past, banks have sued retailers and their vendors in the wake of security breaches, usually resulting in substantial settlements. One of the largest customer information breaches of all time, a 2005 attack on discount retailer TJ Maxx's parent company, TJX, resulted in two dozen lawsuits by numerous banks and credit card companies. Those actions were settled within months of the discovery of the breach.

In another twist, banks could reach beyond Target itself and sue payment processors. There is some precedent for such actions. Following the theft of 130 million credit card numbers in 2008, banks who issued the cards sued processor Heartland Payment Systems, Inc. under several theories, including negligence. A Texas federal court initially dismissed the claims under Texas's and New Jersey's economic loss rules. But, in September 2013, the Fifth



Professional Liability

December 3-4 2015
New York, New York

DRI Publications

Circuit Court of Appeals reversed, holding that the banks' negligence claims could proceed because the financial institutions had no remedy in contract. That case has been remanded. *Lone Star Nat'l Bank, et al. v. Heartland Payment Sys.*, No. 12-20648, slip op. (5th Cir. Sept. 2, 2013).

Finally, other vendors such as software providers, data storage companies, and security consultants could also be liable in actions stemming from Target's breach. For example, when credit card processor CardSystems Solutions was hacked in 2005, Merrick Bank sued CardSystems' security auditor, Savvis, Inc., for negligently certifying that CardSystems had complied with industry standards on cyber security. *Merrick Bank Corp. v. Savvis, Inc.*, No. 2:09-cv-01088-CKJ (E.D. Mo. filed May 12, 2008).

Vendor liability may hinge on the mechanics of the breach, the details of which can remain hazy after the initial attack. In the case of Target, CEO Gregg Steinhafel acknowledged that there was malware installed on Target's point-of-sale registers. That malware may have "scraped" Target's point-of-sale computers for unencrypted customer information. Other sources report that attackers used stolen credentials from a third-party vendor, possibly the company that supplies Target's heating and cooling systems, Fazio Mechanical Services, Inc. and used them to access Target's network. Target has not confirmed those reports, and Fazio has stated that their remote access to Target's network was exclusively for billing, contract submission, and project management.

If true, reports that thieves used passwords obtained from a third-party could trigger a shift in liability. In that circumstance, Target would likely argue that the vendor's weak security—not Target's—is to blame for the breach. Even so, Target may ultimately bear some of the blame. It is possible that a court would find that Target was negligent in granting or managing vendors' external network access.

There will be many lessons learned from the Target breach and subsequent litigation. Customer lawsuits against the primary corporate victims of a cyber-attack are just the beginning. Third-party service providers are also potential defendants in lawsuits brought by customers, financial institutions, and the companies to whom they provide services. The massive scale of the Target breach should be a sobering reminder that even the biggest companies can fall victim to an attack and the litigation resulting from the breach should be monitored closely.

Thomas Hutchinson
Nels Vulin
Bullivant Houser Bailey PC
Portland, Oregon

Back

Coverage B: Personal and Advertising Injury Compendium

DRI Social Links

PDF Version