Bloomberg BNA

Privacy and Security Law Report®

Data Breaches

Cynthia J. Larose, Privacy & Security Practice Leader, Mintz Levin

Views on the Target Data Breach

Target Corp. announced Dec. 19, 2013, that it had discovered an intrusion that may have compromised approximately 40 million customer payment cards used at its U.S. stores from Nov. 27 to Dec. 15, 2013 (12 PVLR 2133, 12/23/13). *The retail giant later said that its investigation of that incident revealed that personal contact information for some 70 million customers also had been stolen* (13 PVLR 61, 1/13/14).

Bloomberg BNA Privacy & Security Law Report Senior Legal Editor Donald G. Aplin posed a series of questions about the Target breach and the company's response to the security incident to Cynthia J. Larose, Privacy & Security Practice leader at Mintz, Levin, Cohn, Ferris, Glovsky and Popeo PC, in Boston. She provided her insights Jan. 15.

BLOOMBERG BNA: Do you see any indication that the hacking breach at Target Corp. was unique or different than other payment card breaches of the last few years?

Larose: There are actually two portions to this incident, although only one is ''payment card'' related. The first that Target went public with was the 40 million compromised credit/debit cards. From what we know through public discussion, it appears that this incident is not very different from the point-of-sale (POS) incidents that have occurred in the recent past, for example, Michaels Stores Inc. (10 PVLR 775, 5/23/11) and Barnes & Noble Inc. (11 PVLR 1584, 10/29/12).

According to Target Chief Executive Officer Gregg Steinhafel, this was related to malware. Although I don't know for sure—and I am not a technical security person—it is reasonable to think that this is a random access memory (RAM) scraper hack.

There is apparently a second piece to this incident that is not typical—the compromise of another 70 million (not accounting for overlap of credit/debit cards) customer names, e-mail addresses, phone numbers and other information. Again, we don't know much about this, but one would expect that this kind of data resided in Target's customer relationship (CRM) system, and a

 ISSN 1538-3423

RAM scraper hack of the POS system wouldn't allow access to the CRM because it wouldn't necessarily give the hacker a path into the corporate network. We have not seen much discussion about this, other than the disclosure by Target, and it certainly adds a different twist to it.

The CRM compromise is still important. It gives ne'er-do-wells all the information they need to launch what could be very effective spear phishing campaigns to wreak havoc.

BLOOMBERG BNA: Given what little Target has revealed about the specifics of the intrusion and theft does it appear there was a problem with Target's compliance with the Payment Card Industry Data Security Standard?

Larose: That is the $40 million—$1 for each record—question. PCI compliance as it stands is not a continuous state—it is a snapshot in time. They could have been PCI compliant Nov. 15 and then Nov. 16 something happened to create a vulnerability. Also, while PCI DSS mandates encryption at various points in the payment process, it does not explicitly require end-to-end encryption (E2EE).

As I understand the technical explanation, because RAM allows the cardholder data (CHD) to pass in clear text for a split second in time, even though the rest of the process may be encrypted, the RAM malware insertion grabs the CHD at the only moment in time it can be read. There are arguments that E2EE isn't the panacea it is touted to be—but for now, it may be the only one available. Heartland Payment Systems Inc. implemented E2EE after its massive malware breach (8 PVLR 204, 2/2/09).

BLOOMBERG BNA: As is the norm in these situations, there have been several consumer class action complaints filed in federal district courts across the country—do you think the putative classes here can establish damages standing and eventually liability?

Larose: I find it interesting that the class actions in the Target breach were filed within days of the incident, without any knowledge of the facts or what Target was or wasn't doing.

I haven't reviewed all of the pleadings, but the ones that I have reviewed don't allege any cognizable harm. There are no allegations of what Target did wrong, because the plaintiffs couldn't possibly have known what Target did wrong, if indeed it did anything wrong.

There is a mountain of precedent here that class counsel will have to climb. Unfortunately for Target—and for every other company in this situation—the law is still developing in this area and we could still have a major development in the facts in the case that could swing in the plaintiffs' favor. Only time will tell, and in the meantime, it is costly for Target.

BLOOMBERG BNA: Target has already given notice that its stockholders should expect lower earnings as a result of the breach, including possible regulator investigations, and several state attorneys general have indicated that they have joined together to investigate the breach—do you think regulatory enforcement actions in court, or through a negotiated settlement, is likely here?

I haven't reviewed all of the class-action pleadings filed against Target, but the ones that I have reviewed don't allege any cognizable harm. There are no allegations of what Target did wrong, because the plaintiffs couldn't possibly have known what Target did wrong, if indeed it did anything wrong.

Larose: If past performance is any indicator of future results, then I would say a negotiated settlement is likely, unless facts emerge that put Target in jeopardy of violation of law or regulations through its operations or its handling of the incident—then you might see direct regulatory enforcement action to make a point.

BLOOMBERG BNA: Target has made a fair amount of information public about their potential losses and costs attached to the breach, given the Securities and Exchange Commission's push to have publicly-traded companies be more transparent in reporting breach costs—should Target also be making these disclosures more formally to the SEC in a Form 8-K or similar filing?

Larose: Since the company has publicly disclosed that the breach could have a ″material adverse effect″ on results of operations, a Form 8-K filing should result.

BLOOMBERG BNA: Target has taken several standard steps to respond to the breach—notifying affected consumers and offering them free credit oversight protection, reassuring customers that they will not be liable for fraudulent purchases, promising data security improvements and apologizing for the breach in advertisements—what else would you tell the Target C-suite it should be doing?

Larose: So far, so good—this is a major incident and a major disruption to the company's business. The CEO's interview on CNBC was quite remarkable—but he needs to be seen on more widely viewed outlets. The majority of Target guests need to see and hear from him.

  PVLR ISSN 1538-3423