Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Home Depot Deal May Spur Banks To Sue Data Breach Targets

By **Allison Grande**

Law360, New York (March 14, 2017, 11:45 PM EDT) -- Home Depot has agreed to fork over more than $25 million to put to bed a proposed class of financial institutions' data breach claims, a move that could prompt more banks and credit unions to go after the retailers that suffered the data breaches rather than pursue more traditional card brand recovery programs to recoup their losses.

The deal was preliminarily approved on Friday by U.S. District Judge Thomas W. Thrash, who set a final approval hearing for Sept. 22. It comes on top of $140 million that Home Depot has already paid to large issuers such as American Express, Discover and others through card brand recovery processes run by Visa and MasterCard for losses stemming from a 2014 breach that compromised 56 million credit and debit card numbers belonging to Home Depot shoppers.

While financial institutions that issued between 70 and 80 percent of the compromised payment cards had agreed to release their claims against the retailer through these recovery programs, the remaining banks and credit unions that decided to press their claims in court ended up getting a potentially better return than the one they would have received had they only pursued the longstanding card brand processes, a result that may inspire others to follow suit, attorneys say.

"The settlement certainly sends a signal that could encourage others to press similar cases, since the financial institutions have gotten a return here," said Brenda Sharton, a Goodwin Procter LLP litigation partner and chair of its privacy and cybersecurity practice. "It's opened the door a crack to the possibility that financial institutions will look to this kind of claim in the wake of data breaches."

Financial institutions are likely to be further encouraged to take the litigation route due to the success that banks and credit unions have had recently with establishing Article III standing. While consumers have largely struggled to show actual harm sufficient to maintain standing in data breach cases, a ruling last year in the Home Depot case that found that the banks and credit unions had alleged a concrete injury to establish standing highlights the easier road that these institutions have had in clearing this obstacle, given that they are usually on the hook for compensating consumers whose cards are compromised as a result of a data breach.

"This goes to show that, as between the cardholders and the banks, it's the banks that suffer the losses," Hughes Hubbard & Reed LLP data privacy and cybersecurity group co-heads Dennis Klein and Seth Rothman said in a joint email.

Dozens of banks and credit unions hit Home Depot with 25 class actions after the retailer confirmed in 2014 that hackers had placed malware on its self-checkout kiosks in stores across the country, allowing them to steal approximately 56 million customers' personal financial information, including names, payment card numbers, expiration dates and security codes.

The financial institutions' cases, which were consolidated in December 2014, alleged that the breach was "the inevitable result" of Home Depot data security practices "characterized by neglect, incompetence and an overarching desire to minimize costs." They claimed the retailer had ignored red flags, expert opinions, employee warnings and industry standards in its repeated refusal to upgrade security, and that their losses from the resulting fraud were in the billions.

The lead plaintiffs — which currently include 50 financial institutions from 44 states, as well as 16 state credit union associations and the Credit Union National Association — chose to press their case despite having available to them the programs that Visa and MasterCard use to assess fraud recovery and operating expense recovery amounts owed to acquiring banks whose merchants suffer payment card security breaches.

"What seems to be happening is that a lot of large issuers seem to go through the MasterCard and Visa processes, while the issuers who press the class action tend to be the smaller ones," Haynes and Boone LLP partner Emily Westridge Black said.

For these issuers, taking the class action route has so far paid off.

The Home Depot settlement marks the second time that financial institutions have launched and ultimately settled claims in the wake of a massive data breach. The first instance drew to a close in December 2015, when Target agreed to pay $39 million to settle claims over a data breach that compromised more than 40 million payment cards used at its stores during a three-week period during the 2013 holiday season.

The Target settlement, which received final approval in May, included a payment of $20.25 million directly to settlement class members, as well as a separate $19.1 million payment to fund MasterCard's card brand recovery process. Eligible financial institutions had the option to make a claim to receive either at least $1.50 per compromised payment card over and above any per-card amount that they had received from MasterCard's or Visa's program, or receive up to 60 percent of their total fraud, reissuance and other costs related to the breach, less any amounts received through the network recovery programs.

The Home Depot settlement, which requires the retailer to place $25 million into a nonrevisionary fund to be distributed to banks and credit unions that have not already released their claims, hinged on similar terms. Under the deal, financial institutions that file a valid claim will be eligible to receive a fixed payment estimated to be $2 per compromised card without having to submit documentation of their losses and regardless of whether any compensation has already been received from a recovery program or another source. Class members that submit proof of losses also are eligible for a supplemental award of up to 60 percent of their documented, uncompensated losses from the data breach.

Both Home Depot and Target have also reached deals to resolve claims by consumers who were impacted by the breach. But those payouts have been considerably less, with the Home Depot plaintiffs snatching $13 million and the Target consumers nabbing a $10 million deal, the validity of which the Eighth Circuit recently instructed the lower court to review.

"The financial institution class action lawsuits have had more success than data breach class actions brought by consumers, or derivative class actions," Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali said. "This is most likely because where the consumer class actions are weak on standing because any credit card fraud is reimbursed by the banks, the banks have nobody reimbursing them. They are often left holding the bag."

Aside from a few notable exceptions, including the Seventh Circuit's decision to revive proposed class actions over data breaches at Neiman Marcus and P.F. Chang's on the grounds that the exposure of their data was enough, consumers have mostly faced an uphill battle to establish standing.

Financial institutions, on the other hand, have had an easier time. In the Home Depot suit last May, Judge Thrash concluded that the financial institutions had pled actual injuries that gave them standing. Home Depot had asked the district court to certify the decision for interlocutory appeal to the Eleventh Circuit, and that appeal bid was still pending when the parties announced their resolution last week.

Similarly, Target reached its deal a year after the district court refused to nix the financial institutions' claims. And financial institutions suing Wendy's over its 2016 data breach continued the emerging trend last month, when a magistrate judge in Pennsylvania recommended that the court allow the plaintiffs' negligence and deceptive trade practices claims to move forward. The fast food giant has asked the district court judge to overturn that ruling.

"Given that the plaintiffs in the Home Depot case were able to overcome the single biggest hurdle there is in privacy litigation, and that's standing, it's not surprising that the case settled," Sharton said.

"This case was unique when it was first filed, in that it was one of the first times in the aftermath of a massive breach that financial institutions became the plaintiffs, and the biggest hurdle was going to be if they have standing," she said. "So once that hurdle was cleared and Home Depot asked for an interlocutory appeal, each side had something to lose, and when that happens, it's a good time to settle."

Besides highlighting the promising recovery potential for financial institutions in the wake of data breaches, the settlement — which the plaintiffs noted in their motion for preliminary approval was recommended by a mediator "after the parties had reached an impasse" and the terms "were only reluctantly accepted" by the litigants — offers other takeaways that could factor prominently in other disputes.

For example, companies that may be the target of a data breach should take note of Home Depot's agreement to pay an extra $2.225 million to cover claims that had been released through the MasterCard recovery program in a process that the financial institutions had claimed was invalid. The sponsors working on behalf of the issuing banks lacked the authority to release claims, and communications sent to the sponsored entities were misleading and coercive, they said.

"That term shows that card companies have to be really careful about disclosures in any communications that they send out," Goodwin counsel Margaret Crockett said.

Home Depot's decision to agree to "implement enhanced security measures to reduce the risk of a future data breach" is also notable, attorneys say. While the retailer pledged to implement new data security measures to settle the consumer claims last year, Thursday's deal takes those commitments a

step further by requiring Home Depot to design and implement reasonable safeguards to identify and manage risks, to develop reasonable steps to select and retain information technology vendors and ensure that they comply with Home Depot's data security practices, and to implement an appropriate industry recognized security control framework.

"As with the Target settlement, there's this nonmonetary component to the settlement that plaintiffs' counsel will likely point to as justifying their fees and the deal," Black said, noting that the settlement states that class counsel are reserving the right to request up to $18 million for their costs and fees, which amounts to less than 30 percent of the sum of the $25 million settlement fund and the amount that the retailer has paid out as part of the card brand recovery process.

"One of the biggest questions has been whether these issuing bank class actions are the best way to resolve these claims, and why do we need this when we have the recovery processes through Visa and MasterCard," Black added. "Getting security concessions from the company is one way that class counsel can say that they got added value from the class action process."

With the gains that financial institutions have made in the Home Depot and Target cases, banks and credit unions are going to continue to keep a close eye on how their recovery prospects in court compare to what they can reap through the card brand recovery processes. They will also be waiting to see how developments such as the recent widespread adoption of what is billed as far more secure chip-and-pin payment card technology, and a looming decision on whether the grocer Schnucks had a duty to protect card information compromised in a 2013 breach, affect their chances.

"This is a space to watch," Black said. "The next few years will really determine whether we'll see a lot of these types of cases and settlements between retailers and financial institutions or whether they'll fade away."

The financial institution plaintiffs in the Home Depot case are represented by co-lead counsel Joseph P. Guglielmo of Scott & Scott Attorneys at Law LLP, Gary F. Lynch of Carlson Lynch Sweet & Kilpela LLP and Kenneth S. Canfield of Doffermyre Shields Canfield & Knowles LLC, and plaintiffs' steering committee chair James J. Pizzirusso of Hausfeld LLP.

Home Depot is represented by Cari K. Dawson and Kristine M. Brown of Alston & Bird LLP.

The case is In Re: The Home Depot Inc., Customer Data Security Breach Litigation, case number 1:14-md-02583, in the U.S. District Court for the Northern District of Georgia.

--Editing by Pamela Wilkinson and Catherine Sum.
