The New York Times | http://nyti.ms/1VjFKbI

BUSINESS DAY

As Online Data Theft Escalates, Banks Look to Retailers to Bear the Losses

By **JULIE CRESWELL** SEPT. 28, 2015

On Sept. 1 last year, the website Rescator, known as the "Amazon.com of the black market," alerted its customers that huge quantities of stolen debit and credit card data would go on sale the next day.

"Load your accounts and prepare for an avalanche of cash!" the website urged.

The next day, two batches of cardholder data were reportedly sold, according to legal documents. The website claimed the cards were 100 percent valid and working. Demand was so high that the website temporarily crashed. Over the next few days, several more batches of card data were sold.

On Sept. 8, Home Depot issued a news release admitting its data systems had been breached.

By then, the damage had been done. Approximately 56 million sets of card data had been stolen, some of which were sold on the black market and remained valid for several days. At a small credit union in California, fraudulent charges of more than $100,000 were posted in just three minutes after the card information was sold on the black market. A bank reported $300,000 in suspicious charges in two hours to the security blog Krebs on Security, which connected Home Depot with the stolen cards before the retailer did.

"With the Home Depot data breach, we weren't even told for days that it existed. That it had happened," said Diana Dykstra, the chief executive of the California and Nevada Credit Union Leagues. "We didn't know that the cards had

been sold on the black market. It hit credit unions and small banks really hard."

A year later, the full tally of the Home Depot data breach remains unknown. Some estimate the fraudulent charges total well into the billions of dollars.

Over the last couple of years, retailing has been a rich hunting ground for online criminals. They hacked into numerous companies, including Neiman Marcus, Sally Beauty and the crafts store Michaels. But the orchestrated theft at Target in late 2013, followed a few months later by the Home Depot data breach, eclipsed all of the others. So far, there have been no arrests in the Target and Home Depot breaches.

As the size and scope of such attacks at retailers has grown, so have the losses, which have been largely shouldered by financial institutions. Now some small banks and others want Home Depot and those companies that suffer data breaches to pay.

One front of the battle is a federal lawsuit winding through the courts, filed by a number of small community banks and credit unions that contend Home Depot long ignored internal and external warnings from security experts that its systems were vulnerable to attack. A similar lawsuit against Target claims that its security protocols were "so deficient that the breach continued for nearly three weeks while Target failed to even notice it." That lawsuit was given class-action status this month by a federal judge in Minnesota.

But even as the lawsuits move forward, retailers are scrambling to meet a deadline to install machines to read E.M.V. microchips — the small metallic rectangles increasingly found on the front of credit and debit cards, named after Europay, MasterCard and Visa, the original backers of the standard. After Thursday, retailers that have not upgraded their systems to read the new chip-enabled cards will be liable for any charges from counterfeit cards.

"Essentially, whoever has the lower level of security will be the one who will be responsible for the unauthorized transaction," said Doug Johnson, a senior vice president of payments and security policy at the American Bankers Association.

For now, that's likely to remain the banks. By some estimates, only 19 percent

of credit and debit cards in circulation will be chip-enabled by the deadline. “It cuts both ways,” Mr. Johnson acknowledged. “If we don’t deploy the chip cards, we maintain the liability that we have currently.”

Retailers and banks are spending billions of dollars to upgrade to the new chip cards. While they hope the cards will slam the door on criminals obtaining financial data that can be used to create and sell counterfeit cards, they warn that other windows for fraud will remain wide open.

“The expectation is that organized criminals are going to move from the physical world to the online world,” said David Robertson, publisher of The Nilson Report, which tracks card industry data.

Credit card fraud losses totaled $8 billion last year, but many consumers may see it as a victimless crime. Certainly there is a high hassle factor around reporting suspicious transactions to the bank or waiting for a reissued card to be mailed, but consumers are generally not held responsible for the fraudulent charges that occur. (Furthermore, experts say while consumers were nervous after the Target and Home Depot data breaches, there is no evidence that they shifted their spending patterns to use cash rather than plastic.)

Instead, a majority of the fraud losses are absorbed by financial institutions, which have become increasingly concerned as the sweep of data breaches at retailers widens.

Historically, when a credit or debit card number was stolen and used to buy goods elsewhere, the banks or financial institutions digested the losses. Then, in cases where the retailer was found to be in breach of security standards, Visa and MasterCard would seek reimbursement for costs associated with the fraud and disburse that money back to the affected financial institutions through a preset formula.

In 2007, for instance, TJX Companies, the owner of T.J. Maxx and Marshalls stores, settled with Visa and others for $40.9 million to cover costs associated with a large data breach.

But small community banks and credit unions say the disbursement of any

money collected from retailers rarely, if ever, makes it to their doors. Most goes to large banks.

"We've not received any payments at all for any fraudulent activity," said Marques Doppler, the chief executive of Profinium, a 140-year-old family-owned bank with four branches in Southern Minnesota and around $350 million in assets. Mr. Doppler declined to say how much Profinium, which is one of the plaintiffs in the Home Depot litigation, lost to fraudulent charges.

For small community banks like Profinium or nonprofit credit unions, a little fraud can hurt in a big way.

"A $100,000 fraud loss to a large financial institution is nothing. But a lot of credit unions have annual net income that is less than $1 million. If you take a couple of big fraud hits, that's substantial for them," said Bill Hampel, chief policy officer and chief economist with the Credit Union National Association.

Moreover, it can cost small banks or credit unions much more to reissue cards involved in a data breach. The average cost to reissue cards affected by the Target breach, according to a survey of banks conducted by the A.B.A. last summer, ranged from $2.70 per card for large banks to $12.75 for banks with less than $1 billion in assets.

So a number of community banks and credit unions filed lawsuits against Target and Home Depot, seeking bigger payouts.

In the case of Home Depot, the lawsuit alleges that the retailer had ignored multiple warnings about its vulnerabilities since 2008. The suit says Home Depot failed to turn on a feature of the 2007 version of Symantec antivirus software specifically designed to spot malware that attacks point-of-sale terminals. Symantec's contractors grew so concerned about Home Depot's approach to security that three of them refused to continue to work for the company and Symantec threatened to cease doing business with Home Depot, according to the lawsuit.

When an employee in 2010 discovered a major security flaw that allowed unauthorized access to Home Depot's network through devices used by its in-store

sales force, the employee was ignored for months. Then he was fired, the lawsuit alleges.

Starting around April 2014, hackers gained access to Home Depot's computer systems using the credentials of a third-party vendor. Targeting the self-checkout registers, the hackers installed malware that siphoned off the information from a payment card when it was swiped on a checkout terminal. The malware remained on Home Depot's terminals for five months, until around Sept. 7, 2014.

Home Depot has broadly denied the allegations. "There's a lot of misinformation out there about this, much of it based on speculation, rumors and opinion by individuals who don't have the facts, and we'll address them in the proper forum," said Stephen Holmes, a spokesman for Home Depot.

But the data breach has been costly for the retailer. In regulatory filings, Home Depot said expenses tied to the breach so far total $232 million, partly offset by $100 million in insurance proceeds.

Lawyers say a good insurance policy will cover expenses related to investigating the data breach, public relations, call-center services and credit monitoring services as well as costs arising from lawsuits.

The challenge for retailers is buying enough of it.

"If you're a retailer, it's hard to buy more than $125 million in coverage in today's market," said Roberta D. Anderson, a co-founder of the Cyber Law and Cybersecurity practice group at the K&L Gates law firm. "Obviously, the potential liability is so much more."

Even as the lawsuit against Home Depot moves forward, the retailer and others are spending billions of dollars — $100 million at Target alone — to upgrade their registers to accept chip-enabled cards. Home Depot says all of its stores will be ready to read chip cards by the Thursday deadline. The retailing giant Walmart says its stores were chip-ready almost a year ago.

Everyone is hoping that the new chip cards will be much tougher for counterfeiters to copy. Among the new security features is a cryptogram, a security code that changes every time the card is used.

But retailers, who have a longstanding feud with Visa and MasterCard over fees, are not happy to be bearing the brunt of the costs to install the new chip readers at their stores (some estimate retailers will spend upward of $30 billion over the next few years) to solve what they see as the bank's problem. Moreover, they say they do not know why the financial industry in the United States is largely issuing chip-and-signature cards rather than the safer chip-and-PIN cards that have been widely adopted in Europe.

"Signature is worthless as a form of authentication" at the point of sale, Mike Cook, an assistant treasurer and senior vice president at Walmart, told attendees during an electronic transactions conference in San Francisco this spring. In the cases of the Target and Home Depot breaches, he said, "not a single PIN debit card needed to be reissued in those breaches. The card number was worthless to the individual thief and fraudsters, because they didn't know the PIN."

The card payment industry argues the new cards will offer better protection against counterfeiting, which they say accounts for the bulk of the fraudulent transactions.

"They also don't want you to have to remember PINs," said Mr. Robertson of The Nilson Report. "The reality of the U.S. market, which is distinct from everywhere else in the world, is that we have an average of 4.5 credit cards per person. That's a lot of PINs to remember."

A version of this article appears in print on September 29, 2015, on page B1 of the New York edition with the headline: After the Break-In, the Bill.
