Nuts and Bolts of Data Breaches and Identity Fraud

By Marcus A. Asner

Data breaches are very much in the headlines these days. It seems that hardly a week goes by without a story about a major new breach, often involving the personal information of hundreds of thousands or even millions of victims. The financial services industry gets hit especially hard, suffering more breaches than any other industry, and often falling victim to identity thieves who exploit the stolen data to steal money.

Marcus A. Asner

So, how do we stop the bad guys? We probably can't – at least not entirely. But banks certainly can take steps to protect themselves. An important starting point, I believe, is to learn how identity thieves actually work: How do they go about stealing data? And how do they exploit the data they've stolen? By gaining insight into how thieves actually operate, we'll have a better chance both to stop the thief before he strikes, and to limit the damage when he does.

IDENTITY FRAUD 101

So how does a fraudster go about committing identity fraud? I served as a federal prosecutor in Manhattan from 2000 to 2009, where I handled a number of big identity fraud cases, and spearheaded the U.S. attorney's office effort to combat identity fraud. My position led me to spend countless hours debriefing identity thieves and getting to know how they worked.

GETTING IDENTITY DATA

Identity fraud ultimately relies on stolen or fictitious identity information. While some fraudsters personally will steal data, many others will trade for it. The Philip Cummings identity theft case, which I handled as a prosecutor, provides a good example. Cummings didn't personally exploit the approximately 30,000 credit reports he stole; instead, he sold reports to others, who used them for fraud. The scheme's impact was dramatic (leading to losses of as much as $100 million), but the market Cummings created for credit reports was tiny when compared to some of the "carding" forums on the Internet. On websites such as Shadowcrew and Mazafaka, criminals openly traded large quantities of identity data, such as lists of card numbers or Social Security numbers.

Where does all this data come from? Sources of identity data can run the gamut from a complex hacking scheme to simply rooting through a victim's garbage (commonly called "dumpster diving"). Low-tech approaches may be the most common. By stealing mail or a purse, a thief may reap a victim's name, date of birth, and address, and perhaps even her account information and Social Security number. A disadvantage of a low-tech approach, of course, is that it's easy to detect, which means the victim could cancel her cards and the thief will risk getting caught.

Data breaches provide a major source of identity data. Breaches come in different varieties. While hacking catches a lot of news, less sophisticated breaches – which might occur when a laptop is lost or stolen – may well be more prevalent and lead to more damage.

Company insiders often cause the most significant breaches. The BetOnSports case I handled provides a good example. Working with an employee in the credit department of a gambling website, the ring stole customers' private identity information, including names, dates of birth, addresses and credit card information. Hospitals are another favorite target. New York Presbyterian Hospital, for example, suffered a large data breach when a patient admissions representative accessed the records of over 40,000 patients.

Data breaches sometimes rely on plain old trickery. A famous example is the ChoicePoint case, where fraudsters opened at least 50 bogus company accounts with a credit reporting agency in the names of phony debt collectors, insurance agencies or other companies, and then used those accounts to steal identities of 145,000 people. Other approaches involve "phishing," "malware" attacks and "pretexting" schemes. The common thread in these "social engineering" schemes is that a thief seeks to trick a person – perhaps a bank employee – into providing identity information.

"Skimming" involves stealing card information by using a card reading device. Thieves may mount a well-disguised skimming device over an ATM, which records the data of cards inserted into the ATM. To capture PINs, thieves might mount a small camera near the key pad, or may use a "PIN overlay pad," which looks like the original pad, but is equipped to record PINs as victims enter them.

EXPLOITING IDENTITY DATA

What does a fraudster do with stolen data? It depends on the scheme. A skimming scheme, for example, may simply involve loading stolen data onto a blank card and withdrawing cash from an ATM. In other cases, however, fraudsters will go to great lengths to build a façade that they are, in fact, the person they are impersonating.[1] By studying carefully government-issued IDs, fraudsters (or their colleagues) often will create authentic looking documents. The thief also may obtain authentic government-issued IDs, for example, by bribing a DMV employee, or by obtaining her victim's birth certificate, and using it to get additional IDs, such as a driver's license or even a passport.

Establishing a fraud address allows fraudsters to receive mail (including utility bills, which can help in getting a government-issued ID) or packages without alerting their victims. A thief can use a friend's address, a neighbor's apartment or a vacant house. Corrupt real estate agents, and mail receiving agencies also are useful sources for fraud addresses.

A thief's next steps depend on the data she has. A stolen credit report can show where the victim already has accounts. To attack an account, the thief often will send a change-of-address letter to the bank or card company. After a few days, the thief might order new checks, or report a lost card and request a replacement. A fraudster also might apply for a new card or credit line with a new bank.

Once a fraudster gets a new card, she can start reaping the rewards. She might start with a test purchase, buying gas, for example, to see if the card is active, while at the same time allowing for a quick escape. If the card works, the fraudster can attempt cash advances or buy expensive merchandise (such as computers or stereo equipment), which she can resell through a fence. A thief also can obtain convenience checks in one victim's name, deposit them into an account established in another victim's name and withdraw funds.

Fraudsters often gain considerable insight about their victims. The Cummings ring, for example, gathered intelligence about security measures, and focused on banks with weaker security (which they believed were smaller banks and banks in rural areas). Ring members also shared intelligence about which retailers ask for identification for credit card purchases, and would buy from stores with weaker security.

The fraudulent purchases or withdrawals often are surprisingly small. This makes sense. A large withdrawal or purchase is more likely to draw scrutiny than a smaller one. By attacking many victims, each on a relatively small scale, a thief still can make a lot of money, while reducing both the risk of getting caught and the likely penalty.

Not everyone is an easy target. Some may have a lower credit rating or their bank may have strong security. A thief nevertheless can exploit almost anyone's identity. One approach, which I call the "bank account daisy chain" method, involves opening multiple accounts in the names of different victims. Then, a thief may instruct the bank of a wealthy victim to transfer funds to a newly-created account. Once the money lands in the second account, he can withdraw some, and transfer funds to multiple other accounts on the daisy chain, withdrawing money along the way, and making the scheme harder to investigate and stop.

RESPONDING TO THE THREAT

Individuals are the first line of defense. Most of us know not to carry around our Social Security cards or birth certificates, to shred sensitive documents, to carry only the ID and credit cards we actually need, and to take care how we handle sensitive documents. It also helps to monitor account statements. At bottom, the rules are simple: (1) know what identity data you have, (2) make sure it's secured so that (a) the bad guys likely won't be able to get it, and (b) if they do get it, your exposure is limited and your most sensitive material remains safe and (3) stay alert for signs that someone is using your identity. And if you do end up a victim, you should take aggressive steps to correct your credit history, and prevent further attacks.

Many of the ways individuals can protect their data also are useful for businesses, although the difference is that corporations typically possess much more data, including data on their employees and customers. The FTC's free guide, "Protecting Personal Information, A Guide For Business," provides useful advice. In a nutshell, businesses need to guard against both low-tech sorts of attacks and more sophisticated hacking schemes – by locking filing cabinets, disposing of personal data appropriately and establishing robust, up-to-date IT security systems. Strong password protocol and computer firewalls are crucial. To guard against a corrupt insider – such as the next Philip Cummings – companies should limit and track which employees have access to sensitive data, and routinely monitor the data that employees access. It also helps to divide sensitive data into separate components, limiting any single employee's access. To limit the impact of any breach, businesses need to understand fully what data they have, and keep only the material they actually need. Financial institutions also should routinely reevaluate their data security, looking for vulnerabilities and fixing them as they arise. And banks can fight social engineering schemes with employee training, clear and enforced rules articulating the information employees may provide over the telephone or the Internet and monitoring interactions with customers.

How do banks protect the money and other valuables they hold? Knowing how identity thieves actually operate will help. Remember, one of the first things an identity thief often does is change the victim's address. So change-of-address letters can be red flags. Banks can help thwart identity theft by contacting the old email address or phone number, and notifying the victim of the change. Banks also can develop programs to look for unusual moves or purchasing activity. Here's an example from my own life: I'm a lawyer in New York, but a few years ago I found myself in Oklahoma and decided to buy some cowboy boots. My credit card company recognized this as unusual (it was), and immediately called my cell to determine if the transaction was real. Banks also can protect their online customers by recognizing commonly used computers, establishing better password protocols and asking customers non-obvious security questions. Banks also limit the damage from attacks by imposing limits on the withdrawals permitted through vulnerable access points such as ATMs.

Finally, financial institutions need to plan for the worst. Companies hit with a data breach often face a dizzying array of practical and legal issues, ranging from investigating and stopping the breach, to interfacing with law enforcement, complying with victim notification requirements, dealing with the press, and defending civil litigation. Having a plan to address a security breach – such as a plan to change customer passwords, disconnect the IT system from the Internet, and timely notify victims – and taking the time to go through table top "fire drill" type exercises, can go a long way toward helping banks execute an effective response and minimize the impact of any breach. ■

Marcus Asner is a partner at the New York office of Arnold & Porter. Asner is a trial lawyer in the firm's white collar practice group and co-chairs the privacy and data security practice. Asner has extensive experience with data breaches, cybercrime, corporate espionage, money laundering and bank fraud matters. He can be reached at Marcus.Asner@apks.com or (212) 836-7222.

FOOTNOTES

1. The District Court's opinion in the Cummings matter provides a useful description of how one identity theft ring went about exploiting stolen identity data. *United States v. Abiodun*, 442 F. Supp. 2d 88, 90-94 (S.D.N.Y. 2006), aff'd in pertinent part, 536 F.3d 162 (2d Cir. 2008).