

[ABA Journal - Law News Now](#)

ABAJOURNAL
Law News Now



[Home](#) » [Magazine](#) » [March 2006](#) » Stolen Lives

Cover Story

Stolen Lives

Victims of Identity Theft Start Looking for Damages from Companies That Held Their Personal Financial Information

March 2006 Issue

By Jason Krause

[Comments: 0](#)

[E-mail / Share](#)

[Permalink](#)

[Print](#)

[Reprint](#)

The most vulnerable victims of identity theft are the people whose personal financial information is stolen. For them, identity theft can wreak havoc with their lives, even though federal and state laws limit their liability for charges made in their name that they can prove were fraudulent.

But proving that kind of fraud by anonymous, invisible thieves who commit most of their crimes electronically is a difficult task. And individuals are usually on their own in trying to repair the damages from identity theft. The San Diego-based Identity Theft Resource Center estimates that it takes the average person 175 hours and \$800 to repair the mess caused by an instance of identity theft. Under current federal and state laws, individuals have little recourse to seek damages for their losses.

In the cold, objective eyes of the law, the primary victims of identity theft are often not the individuals whose personal financial information is stolen. Rather, they are the financial institutions and businesses in possession of that information when it was stolen. As crime victims themselves, financial institutions and retail companies have largely been shielded from responsibility for losses to individuals when information is compromised.

But as identity theft continues to grow, questions are being raised about whether financial institutions and businesses should have that protection.

“If someone has to spend time and money trying to recover their identity, how can there be no damages?” says Jon Stanley, a lawyer in Cape Elizabeth, Maine, who practices in the areas of privacy, information security and cybercrime. “The question becomes, ‘Does a third party, that is, someone whose information is stolen, have recourse?’ Companies tend to think of it as their information about you, not your information.”

But things may be changing. More attention is being focused on the legal responsibilities of businesses that handle personal financial information about individuals, and whether those businesses should have some liability when that data is lost or stolen. Increasingly, consumer watchdogs, lawyers, regulatory agencies and even members of Congress are pushing in that direction.

And if push comes to shove, it could change the way identity theft is handled in the United States and perhaps other countries, as well.

Don't Talk

Identity theft--where information like social security and credit card numbers are stolen from individuals and used by thieves for their own purposes is really nothing new.

Criminals have always had ways to get information about other people, even if it meant stealing wallets or digging through Dumpsters. But the Internet, along with widespread electronic sharing and storing of data, has made the crime more pernicious. Identity thieves often manage to steal millions of pieces of information from online sites, and they use the Internet to sell that information, make illegal purchases and obtain fraudulent loans. In extreme cases, the victims may feel that their own identities have practically disappeared under the onslaught of the theft.

Just measuring the scope of the identity theft problem is difficult. One source of statistics is the Federal Trade Commission. In 2005, the commission received 255,565 consumer reports of identity theft, an increase of 8,718 over the number of identity theft reports it received in 2004.

Those numbers may not reveal the true scope of identity theft--or at least its potential scope--because financial institutions, data processing firms and retail businesses are reluctant to discuss incidents in which its customers' personal financial information may have been stolen, lost or otherwise compromised.

"I just don't see any advantage to our speaking about this issue," a spokesman for JP Morgan Chase, one of the nation's largest financial institutions, told the ABA Journal. For a long time, companies were able to avoid reporting breaches of their electronic data banks. As a result, many consumers never knew that their credit card numbers or other personal and financial information might be in the hands of identity thieves.

But recently, some companies have admitted that they lost personal information belonging to millions of customers. In 2005, for instance, ChoicePoint Inc. in Alpharetta, Ga., notified some 140,000 customers that their data had been stolen, and CardSystems Solutions in Tucson, Ariz., announced it may have lost credit card records for as many as 40 million people.

On Jan. 26, the FTC announced that ChoicePoint will pay a \$10 million fine, the largest ever levied by the commission. The company also will pay another \$5 million to compensate customers for losses stemming from the data breach. The FTC estimates that information on 163,000 individuals in the United States was compromised, and that there are now some 800 actual victims of identity theft as a result. The company's estimates are lower.

One of the triggers for that new openness is a 2003 California law that requires businesses to notify residents of that state when they have reason to believe that personal financial records about those residents have been accessed or acquired by unauthorized parties.

In hearings held last year by the U.S. Senate Judiciary Committee, executives from ChoicePoint and LexisNexis acknowledged under questioning by Sen. Dianne Feinstein, D-Calif., that they had not notified some victims of identity theft before the California disclosure law went into effect.

A Changing Landscape

California's public disclosure law is quickly changing the legal landscape around identity theft. Once the law went into effect and businesses began sending thousands of letters to identity theft victims in California, lawmakers and law enforcement officials elsewhere began asking the obvious question: Had their constituents been victimized, too? Attorneys general from a number of states sent demand letters to businesses like ChoicePoint hoping to force the same disclosures for their constituents that Californians received.

A spate of legislative proposals at the federal and state levels also has followed the recent disclosures of compromised personal financial information held by companies. As of early February, 21 states had adopted general laws mandating notification of affected residents by companies that experienced data security breaches since the California measure was passed in 2003, according to William B. Baker, a lawyer in Washington, D.C., who is co-chair of the E-Privacy Law Committee in the ABA Section of Science and Technology Law.

The outcome of this furious bout of legislating has been a hodgepodge of state laws that impose different requirements on businesses for reporting data security breaches to customers. California, for instance, allows businesses to notify customers with radio announcements rather than letters if more than 500,000 people are affected. In Connecticut, that threshold is 100,000.

California's law has been criticized for being too burdensome on businesses, so some states have crafted very limited or narrow laws. Georgia's law only applies to "information brokers," companies that collect and sell consumer data. Indiana's notification law applies only to state government agencies. Colorado doesn't mandate notification, but allows individuals to freeze their credit ratings if they believe identity thieves may have stolen and misused their data.

Meanwhile, there are several legislative proposals in Congress to create a national rule for public disclosure in the event of a breach of personal financial information at a company, but none has come close to passing.

Two Senate bills would require a company to notify consumers nationwide if the company finds personal information is stolen. The bills also set minimum security standards for businesses. One bill, introduced by Sens. Arlen Specter, R-Pa., and Patrick Leahy, D-Vt., also would create new regulations for companies that are classified as data brokers. The bill would restrict the sale of information like Social Security numbers and mandate that individuals be allowed to get copies of personal information held by data brokers.

There is debate among consumer advocates over whether action by Congress would be beneficial at this time. Some argue against congressional action on grounds that the proposed federal measures are weaker than some state laws already in effect. Others disagree, arguing that one federal law regulating public disclosure of data security breaches would be a welcome development.

Baker says he advises clients that the first issue is to determine the nature of the security breach because identity theft is not always the purpose. "Did someone clearly steal private records, or did someone just misplace some storage tapes?" he says. "Often, a laptop computer is stolen not for information, but for parts. If a laptop is found two days later missing key components, you can probably assume it wasn't about identity theft."

But if there was a data breach, Baker says it's better to respond openly regardless of whether there is controlling law. CardSystems suffered such bad publicity when hackers broke into its system that its customers began leaving, and it was driven to the brink of financial ruin, he notes. "One thing I've found is that companies need to act very proactively, to announce these things and try to minimize bad publicity. You can't try to ignore the problem anymore."

The FTC Asserts Itself

While Congress ponders legislation, the Federal Trade Commission has become more active in enforcing privacy rules for businesses, primarily in accordance with the Financial Modernization Act of 1999, known as Gramm-

Leach-Bliley for its primary sponsors. The law mandates that financial institutions--which are defined rather broadly--adequately protect the personal financial information about customers that they hold. A safeguards rule in the act requires all companies defined as financial institutions to design, implement and maintain safeguards to protect customer information. Those companies also must publish information on such things as whether they encrypt data and how long they keep customer records.

Meanwhile, however, the FTC recently settled lawsuits against two companies that are not financial institutions in the traditional sense.

In June 2005, the FTC fined BJ's Wholesale Club, based in Natick, Mass., for lax handling of customers' personal financial information. The FTC claimed that BJ's failed to take steps to defend its computer systems, making it easy for criminals to access customer records.

Then in December, the FTC won a similar settlement against DSW, a Columbus, Ohio-based shoe retailer. The FTC said DSW kept consumer records in an unsecured system that made it possible for identity thieves to steal credit card information.

Along with the fine levied against ChoicePoint in January, those actions suggest that the FTC views thwarting identity theft as a duty for businesses regardless of whether the provisions of Gramm-Leach-Bliley directly relate to them. Moreover, the commission claims broad authority under section 5 of the FTC Act (prohibiting unfair or deceptive practices) to take action against companies that engage in lax security practices that could expose the personal financial information of customers to theft or loss.

"Unless you're one of a few businesses that are exempt from our jurisdiction, like insurance companies, we will act against businesses that fail to protect their customer data," says Betsy Broder, assistant director of the FTC's newly formed Division of Privacy and Identity Protection. (The division will focus on data security, credit reporting and Gramm-Leach-Bliley enforcement cases.)

While the FTC did not file the actions against BJ's and DSW under Gramm-Leach-Bliley, Broder says all businesses should look to that law for guidance on how to protect consumer data. At a basic level, she says, that means businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan.

Many large businesses entrust such planning and execution to a chief technical officer or chief privacy officer. Broder says she understands that most small businesses cannot be expected to hire a full-time privacy specialist, but she adds that all businesses must be able to show they have a security plan in place.

"We're not looking for a perfect system," Broder says. "But we need to see that you've taken reasonable steps to protect your customers' information."

Some remedies are available to individuals under various federal and state laws that apply to identity theft.

Under the federal Fair Credit Reporting Act, individuals have the right to see their credit reports for free every year, which can help them identify fraudulent accounts or charges. If someone suspects charges have been made, it is possible to put a fraud alert on the credit report. An alert gives the person 90 days to try to clear up fraudulent activity without damaging his or her credit score. If he or she can prove fraud, it is possible to add an extended alert for seven years, which means businesses have to verify that person's identity before extending credit during that time. In extreme cases, it is possible to apply for a new Social Security number.

Unfortunately, proving credit fraud is often difficult, and people often spend years trying to clear their names or wind up suffering financially. The FTC offers help to individuals by providing online forms like affidavits to submit to credit agencies reporting identity thefts.

In January, Illinois Attorney General Lisa Madigan announced that she will commit two full-time staff members to helping identity theft victims repair their credit histories. Madigan says her office will be the first in the United States to offer full-time help to identity theft victims. (According to FTC figures, Illinois had 11,138 identity theft cases in 2004, the fifth-highest number in the country.)

Contradictory Case Law

But perhaps the thorniest identity theft question is whether an individual should have a private right of action against businesses when his or her personal financial data is stolen, lost or otherwise compromised.

Some legal experts believe such actions would force more financial institutions and businesses to handle personal data more carefully. The Computer Fraud and Abuse Act, the federal law that typically serves as the basis for prosecutions that follow computer break-ins, has a civil suit provision, but it has been interpreted very narrowly by most courts.

The case law on the liability issue is somewhat scattered and contradictory. Some federal courts have rejected efforts by individuals to bring civil actions against financial institutions and other businesses under the computer fraud act. But, Baker says, "It's pretty hard to maintain a claim because it's hard to show damages. It's also very hard to trace causation--how do you prove unauthorized purchases are tied to a specific instance of identity theft?"

One of the few cases expressly addressing whether a business can be held liable under the computer fraud act for breaches of personal information is *Doe v. Dartmouth-Hitchcock Medical Center*, No. CIV. 00-100-M (D.N.H. July 19, 2001), an unreported case. There, a doctor had intentionally gained unauthorized access to medical records belonging to a woman with whom he had a personal relationship. But the court said that even though the doctor violated the woman's privacy by viewing her computer records, it did not hold the doctor's employer liable, on grounds that there was no criminal intent.

One of the key arguments made by the defendants was that they can hardly be held liable for computer crimes when they also are victims.

There was a similar result in *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004), where two employees of a cable manufacturer were allegedly induced to steal large volumes of confidential computer records for a competitor. The court ruled that because the plaintiffs could not prove a loss, they had no cause of action under the computer fraud act.

But the San Francisco-based 9th U.S. Circuit Court of Appeals did recognize a cause of action under the computer fraud act and the Stored Communications Act in a case where plaintiffs alleged that an Internet provider willfully exposed the content of their e-mails over the Internet. *Theofel v. Farey-Jones*, 359 F.3d 1066 (2004). The 9th Circuit remanded the case to the district court, which had previously ruled the plaintiffs had no right to sue, for further proceedings.

More recently, a federal district court held that a plaintiff could proceed with a case seeking damages on grounds that the defendant intentionally violated the plaintiff's personal information. *Charles Schwab & Co. Inc. v. Carter*, No. 04 C 7071 (N.D. Ill. Sept. 27, 2005).

The facts alleged in *Carter* are fairly common for identity theft cases: An employee leaves one company, takes confidential information off the computer system and brings it along to a new job with a competitor. Acorn, the company that hired the employee away from Schwab, argued that Schwab had no cause of action under the computer fraud act. The court disagreed, stating that the defendants, unlike those in *Dartmouth-Hitchcock Medical Center*, had actively coerced individuals to steal information, making them potentially liable.

Despite some of the recent outcomes in these cases, legal experts say it will take new federal laws to make civil

remedies realistic for identity crimes.

Baker says such a law would have to allow courts to presume causation between the theft of personal data and the exploitation of that data for financial gain. Otherwise, it may be impossible to ever prove that a computer break-in led to actual damages. Another approach would be to impose fines or penalties on companies that allow a data theft to occur through lax security practices.

Unless new remedies are enacted, experts say, it may be impossible for individuals to pursue actions against any defendants but data thieves who are caught in possession of stolen personal data.

The Fight Goes On

Law enforcement agencies continue to attack identity theft on the criminal law front. But because identity theft can happen anywhere on the globe, it is unlikely police can ever completely contain the problem. Moreover, law enforcement officials say they often lack adequate resources and coordination to deal with the problem.

And in some cases, police agencies have higher immediate priorities than identity theft, says Kimberly Peretti, a trial attorney in the Computer Crime and Intellectual Property Section of the Justice Department.

Police often treat identity theft as a “precursor crime,” especially in conjunction with drug crimes, Peretti says. “Often, police will make a drug bust, and there will be identity theft evidence all over the place, but that’s not the priority, so they ignore it.”

Meanwhile, identity thieves continue to find new ways to pursue their crimes. One of their latest gambits, Peretti says, is to use stolen personal financial information to buy gift cards or prepaid debit cards, which are harder to track than credit cards.

Identity thieves even have turned to blackmail. Late last year, computer hackers informed White Wolf Publishing, which makes role-playing video games, that they had stolen passwords and identifying information about customers.

When the company refused their demands for a ransom to get the information back, the hackers responded by e-mailing individual customers to tell them they could buy their stolen information back for \$10.

In recent years, consumers have become more aware of the threat that identity theft poses, and public outcry has pressured legislators to do more about the issue. But it may take even more pressure to spur companies to plug the security holes that help make identity theft possible.

“Unfortunately, it will probably take more push back from consumers before we see more effort to fix this problem,” says Erin Kenneally, CEO of Elchemy Inc., a technology company in LaJolla, Calif. The company is working with the National Institute of Justice, a research arm of the Justice Department, to develop ways in which various law enforcement agencies can link their resources for investigating identity theft cases.

“We’re dealing with a crime wave, the scope of which we’re not sure of, and victims who have reasons to cover up the extent of the crime,” Stanley says. “It hasn’t stopped politicians from trying to do something, but they are doing it on incomplete information. We don’t even have a good definition of what identity theft is. We don’t know the nature, character and extent of the problem.”

Jason Krause is a legal affairs writer for the ABA Journal.

[Comments: 0](#)

[E-mail / Share](#)

[Permalink](#)

[Print](#)

[Reprint](#)

Comments

- [Report Abuse](#)

Be the first to comment.

Commenting has expired on this post.

Copyright 2008 American Bar Association. All rights reserved.