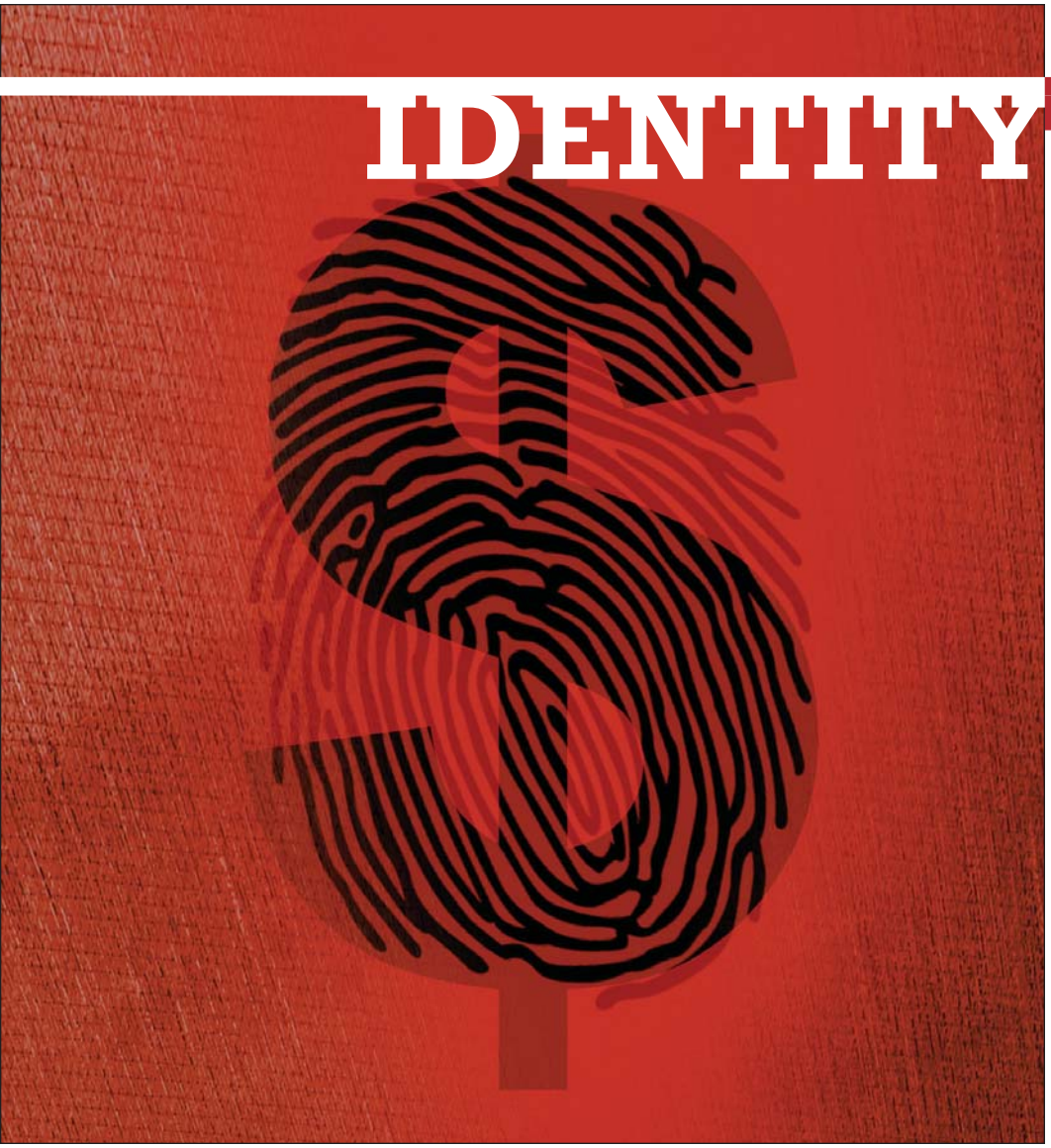


IDENTITY THEFT

Greater credit options have increased consumers' financial flexibility — and the ability of criminals to steal information. Still, the share of people victimized remains small

BY BETTY JOYCE NASH

When Lisa Cook of Columbia, S.C., tried to open her first checking account, somebody had already beat her to it, using her Social Security Number but a different name.

"It was $600-some in the red," Cook says. That was the first of about $98,000 in debt amassed under her Social Security Number. Cook, who is 26, was one of 2,148 people in South Carolina reporting identity theft to the Federal Trade Commission in 2004, roughly a third of them between the ages of 18 and 29.

After more than a year of fending off bill collectors, navigating voice-mail mazes for credit reports, making investigative trips to the imposter's town, copying fees, frustration, and heartache, Cook is repairing her financial records.

"I was building my own credit," says Cook. "My mom told me if you don't have credit, you don't have anything." The imposter was eventually caught, charged, and imprisoned.

Assimilation of personal data has been a useful tool in allocating credit — let's face it, your Social Security Number is recorded and used as an identifier by everyone from doctor to landlord to employer. The data are a prime target for resellers as well as thieves, and have become relatively easy to mine.

Between electronic records and the ubiquity of credit cards, it's not so shocking that financial crimes would blossom. And for the fifth year in a row, identity theft was at the top of the FTC's fraud complaint list. But what is identity theft? Does it include plain old credit card thievery? If so, survey data indicate that there were about 10 million victims in 2003. Or is it something larger — like using a person's Social Security Number to establish new accounts?

The challenge facing financial institutions and regulators alike is finding the proper balance between protecting consumers and making credit readily available. Nobody wants to hamper the efficient credit market that the free flow of data has created. But as online transactions and services grow, consumers, banks, and regulators are paying closer attention to identity theft and the mounting cost of

PHOTOGRAPHY: GETTY IMAGES

LEGISLATIVE AND REGULATORY ACTION

The Identity Theft and Assumption Deterrence Act of 1998

- Makes ID theft a federal crime with penalties of up to 15 years and a maximum fine of $250,000
- Establishes victim status so he can seek restitution if there is a conviction
- Establishes the Federal Trade Commission as the central agency to collect complaints, referrals, and resources

Gramm-Leach-Bliley Act of 1999

- Requires financial institutions to protect information collected about individuals
- Requires financial institutions to give consumers privacy notices that explain the institutions' information-sharing practices
- Gives consumers the right to limit some information sharing

Fair and Accurate Credit Transactions Act of 2003

- Requires account numbers on credit card receipts be truncated to prevent confiscation of names and numbers
- Requires major credit-reporting agencies to provide consumers with a free copy of credit report annually
- Permits victims of ID theft to place an "alert" on credit files
- Rule making in progress

SOURCES: Federal Trade Commission and Privacy Rights Clearinghouse

preventing it. The crime has spawned its own industry of solutions and consultants, including identity theft insurance.

The Costs of ID Theft

Overall, identity theft cost businesses and financial institutions $52.6 billion in 2004, according to a Javelin Strategy and Research survey. And that's just money lost; that doesn't count the complex systems put in place to fight it. Javelin is a consulting firm for the financial services and payments industry. The survey, similar in methodology to the FTC's 2003 Identity Theft Survey Report, was sponsored by financial services firms, including Visa USA and Wells Fargo Bank. The survey polled 4,000 people, including 507 fraud victims.

It's important to distinguish between credit card fraud and true identity theft, cautions John Hall, a spokesman with the American Bankers Association. "It's the difference between crime and murder," he says. "You don't just lump them together."

Fraud involving general-purpose credit cards averages less than 0.06 percent of sales today, thanks to sophisticated detection and monitoring. Merchants who do business online report decreases in lost revenue from payment fraud, from 3.6 percent in 2000 to 1.8 percent in 2004. Federal law limits consumer liability to $50 per card.

Account takeover or new account fraud, like Lisa Cook's, is more troubling and a major hassle for the victim. Thieves steal what's in the account and use a creditworthy identity to get more; often their victims are relatives. Not always, though. Lisa Cook's imposter was as different from Lisa as night is from day — in sex, race, age, and residence. He was able to get credit at stores where she was not. And he bought two cars, got a business license, and several loans from payday lenders.

Credit Where Credit Is Due

Economists view credit favorably. It gives people greater financial choices and allows them to "smooth" their consumption patterns over time. The growth in affordable, available credit stems largely from the flow of personal data in the national credit reporting system. The information provides lenders with many pieces to evaluate who gets credit and who doesn't and, most importantly, to reduce uncertainty and price the credit according to risk. Economists William Roberds of the Federal Reserve Bank of Atlanta and Charles Kahn of the University of Illinois have studied credit and identity theft and recently published a working paper about it.

"Any successful payment system, credit card ... cash or whatever has to have some way of tying the person in the transaction to somebody's records," Roberds says in an interview.

While instances of identity theft enrage consumers, no doubt about it, regulators are thinking long and hard before imposing strict rules on the data-gathering activities. According to Roberds and Kahn: "This reluctance stems, in part, from the notion that the collection of personal data is essential to the process of allocating credit."

Society may ultimately have to decide on a rate of identity theft that balances its preference for privacy with its tolerance for transaction fraud, the authors say.

"The take we have on credit card fraud, identity theft, is that it's sort of the byproduct of something good," Roberds says. "The something good is the fact that credit cards and debit cards and other types of payment systems have a good feature, allowing merchants to share identifying information on you."

By virtue of the fact that you have a credit card, your credit record is tied to you and allows you to engage in transactions you otherwise might not — that's the good side. "But the bad side is, once a mistake is made, once somebody gets a hold of your credit card number and uses it to tie you to transactions that they're involved in, that's a down side of that system," Roberds says.

Roberds and Kohn created a model that showed the upside outweighs the downside. "That's pretty much the way

it's worked out in the real world," Roberds says. "We worry about identity theft, but we don't want to give up our credit and debit cards."

The model indicates that in an economy where information is shared and there are more buyers, there is also more provision of credit. "People would be generally better off than in an economy where you didn't have this information sharing," he notes.

Credit has lowered the cost to merchants to do business on credit and likewise cut the cost to them of providing credit to customers. "It's expanded the set of transactions that can be done on credit," he says. "But the downside is we have these two prevalent types of fraud that have to be kept in check."

The Buck Stops Here

Worrisome data losses in 2005 among businesses, including several banks and data firms, set off a wave of publicity that raised questions about the security of personal data. Charlotte-based Bank of America lost a backup tape with information on 1.2 million accounts, and Bank of America and Wachovia, among other institutions, also lost data through dishonest insiders, according to Privacy Rights Clearinghouse, which maintains a list of data breaches.

Bank of America and Wachovia say they notify customers if data have been compromised. Among Fifth District states, North Carolina alone requires notification in case of data breaches, as of Dec. 1, 2005.

While the losses are undesirable, Julie Davis, spokeswoman for Bank of America, says that as far as the bank knows, none of the information has been used. "So while the tapes were lost, it really was a case of lost tapes and not stolen data."

The banking industry has come a long way since about 2000 when banks were afraid to "even mention the words 'identity theft,'" according to Ariana-Michele Moore, a senior analyst at Celent, a financial services consulting firm. Banks today are educating consumers and employees, monitoring transactions, and using complex and expensive software systems to pick up the latest cyber scams. They sometimes offer free services to identity theft victims, such as account monitoring.

But they can't reveal all their tactics, says Nessa Feddis, senior federal counsel at the American Bankers Association. "The banks do a lot more than what we can say," Feddis says. After all, they don't want to publish a road map for criminals.

Steve Scott, Wachovia's director of corporate information security, says that when credit card numbers get exposed somehow online, "not only do we have to deal with the fraudulent activity that comes with those cards but we also have to deal with the customer."

While banks can't discuss nuts and bolts of preventive strategies, they've ramped up responses as the threats have escalated. Those include everything from the simplest and cheapest consumer and employee education to thorough investigation of partners.

Wachovia sends teams to supplier sites to review security. "Then we measure that against our own standards and requirements," Scott says. "If there are gaps, then we work with those vendors to close that gap and those could be deal breakers."

Scott won't say how big a problem identity theft is at Wachovia. "We all know it's a problem and we've had to rise to meet that ... the identity theft creates more work for us." In general, he says, "there's a lot more energy being put around knowing the customer, a lot more process being put in place to make sure we have valid identification." A delicate balance exists between security and convenience. "Customers still want services that are dependable, available, secure, and easy to use," Scott says. Sometimes that's a hard combination. Customer acceptance and usability are the biggest drivers.

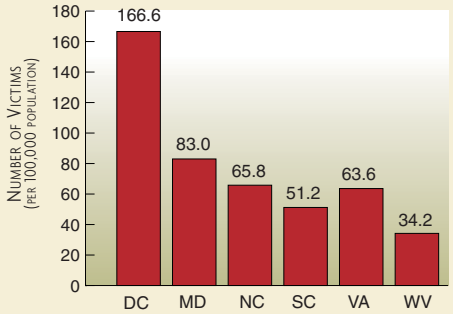
The Federal Financial Institutions Examination Council, comprised of representatives from five agencies including the Federal Reserve, has told banks by the end of 2006 to complete a risk assessment and implement any technology necessary for added security, including customer authentication, verification of new customers, monitoring, and reporting.

"We, like the other financial institutions, are going through that assessment activity as we speak," Wachovia's Scott says. "Based on that, we'll use that information to apply the appropriate controls to where we think it needs to be best implemented." He would not say how much the extra actions would cost.

Bank of America, with the biggest pool of online customers nationwide, about 14 million, in 2005 introduced SiteKey. Spokeswoman Davis says it had been in the works for two years. SiteKey customers choose from among thousands of images and then create a phrase unique to them. They also select from a list of challenge questions. When logging on, customers look for the icon and phrase to pop up and then enter a password. "If you're at another computer, it asks you a challenge question," Davis explains. "The bank validates you before you log on. It lets the customer know they have indeed reached Bank of America." Even if an ID and pass code have been stolen through spyware (malicious software that can take over certain computer operations without the user's knowl-

Identity Theft Victims By State

The District of Columbia's rate of identity theft is the highest in the nation. Credit card fraud, at 28 percent of all cases nationwide, is the most common form of reported identity theft.



SOURCE: Federal Trade Commission

edge) or e-mail scams that link to bogus Web sites, the account would be unavailable to an imposter.

Davis, like Scott of Wachovia, would not discuss how much SiteKey has cut into the bank's bottom line or how big a problem identity theft is for Bank of America.

Even with risks associated with spyware, consumers might do well to bank online, along with 44 percent of all Internet users and 25 percent of adults who now do so. "Because I'm logging onto my account daily or weekly, I would be the first to notice, 'Gee, I didn't write that check,'" says Celent's Moore.

Still, cyber crimes are increasing and that is expected to slow e-commerce growth rates by 1 percent to 3 percent, according to Avivah Litan of the information technology research firm Gartner Inc. Phishing attacks, for example, reached an estimated 73 million U.S. adults in the 12 months ending May 2005, a 28 percent increase over the previous 12-month period.

Social Insecurity

While data dissemination and malicious Web work has driven identity theft, most thieves still get their information the old-fashioned way. In cases where the method was known, the Javelin Survey reports 68 percent of information was gleaned offline compared to 11.6 online. The most common methods include lost or stolen wallets, misappropriation by family or friends, and mail theft. That's how Lisa Cook's imposter got her Social Security card — her wallet had been stolen.

It's no wonder that Social Security Numbers as identifiers have come under increased scrutiny. "It's overwhelming when you look at the big picture of identity theft and the opportunity," notes Ariana-Michele Moore of Celent, referring to peoples' relationships to organizations. Between landlords, employers, background checks for even volunteer work, it's important for people to realize how available their personal information may be.

Social Security Numbers (SSNs), names, and birth dates, are the prized identifiers for identity thieves, according to the U.S. Government Accountability Office in reports in 2004 and 2005 that examine the exposure of SSNs. The numbers were first used in 1936 to track workers' earnings, but now SSNs are collected widely. The GAO reports the numbers are often available in public records, especially state and local government records. The GAO reported in 2004 that state agencies in 41 states and the District of Columbia displayed SSNs in public records. This was also true in 75 percent of U.S. counties. It has been used on drivers' licenses and insurance cards, including Medicare and government- issued insurance cards.

Data resellers, credit reporting agencies, and health care organizations use SSNs. Information resellers may obtain the numbers from records, including court records such as bankruptcies, real estate transactions, voter registrations, and professional licenses or from business clients. In 2003, the GAO investigated Internet-based information resellers to determine what information might be available. The investigators paid fees and supplied several resellers with legitimate SSNs, and in return received information based on those numbers, such as a name, address, telephone number. During the investigation, none of the Internet-based resellers bothered to verify who they were or whether they were using the information for the purpose they'd indicated.

As Lisa Cook discovered, if a thief has your Social Security Number, he's got a good head start on fraud. Twenty-nine percent of identity theft victim complaints in 2004 came from people aged 18 to 29, according to the FTC. In the European Union, identity theft isn't as big a problem, and some experts have suggested it's because Social Security Numbers aren't universal identifiers. In Europe, residents have national identity cards and Social Security Numbers are used solely for retirement benefits. Privacy laws keep businesses from sharing and selling personal or private financial information. Of course, the price they pay is slower credit decisions.

But some "red flag rules" are coming, under the Fair and Accurate Credit Transactions Act, the law passed in 2003 that gives consumers one free annual credit report for the asking.

Lisa Cook is still asking herself how the thief got away with using his name with her number for so long. She'd built up a good report by paying her bills on time.

"I already had stuff on there [credit report], but it was all good, until he came along." **RF**

Readings

Bovbjerg, Barbara D. "Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain." Government Accounting Office Document GAO-05-1016T, September 15, 2005.

Cheney, Julia S. "Identity Theft: A Pernicious and Costly Fraud." Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 03-18, December 2003.

Duncan, Joseph W. "Congress Faces Critical Decision About Consumer Credit Legislation (The Fair Credit Reporting Act of 1970 and 1996)." *Business Economics*, July 2003, vol. 38, no. 3, pp. 62-71.

Kahn, Charles M., and William Roberds. "Credit and Identity Theft." Federal Reserve Bank of Atlanta Working Paper 2005-19, August 2005.

"National and State Trends in Fraud & Identity Theft, January - December 2004." Federal Trade Commission, February 1, 2005.