



# In Focus



## Identity crisis

**T**Hese days, it seems you have to guard your personal data for fear that someone may steal your identity. For example, you buy concert tickets over the phone. But how do you know the customer service rep you just gave your credit card number to won't use it to buy some bling? You hire a baby sitter for the evening. But how do you know she won't rifle through the financial records in your home office and uncover your Social Security number? You toss out those annoying applications for credit cards. How do you know someone won't dig through your trash, find them, and apply for credit in your name? Well, you can't live in a bubble, but you can take precautions. In the following pages, you'll hear from a Rotarian whose identity was stolen (J. Michelle Sybesma, pictured here); find out how to protect sensitive information at work; and learn what to do if you ever become a victim of identity theft. So the next time you get your Visa bill and discover that you supposedly bought a \$5,400 pair of diamond earrings from Tiffany & Co., you'll know what to do. >>



## To catch a thief

*A Rotarian tries to find out who stole her identity*

by Dean Rea

The light gray couch would fit perfectly in her living room, Jamie Michelle Sybesma thought as she walked through a furniture store in 1994. She was 22, had recently landed a job at an Indianapolis hotel, and had paid off all her bills. She decided to buy the couch on credit because the store offered interest-free monthly payments.

A salesperson said the store could arrange financing but wouldn't be able to issue a large line of credit. There were too many inquiries on her credit report, the clerk said. Lenders had been asking credit bureaus for copies of Sybesma's report to verify information about her on credit applications before issuing cards in her name.

But Sybesma hadn't been applying for credit cards.

"There's got to be a mistake. What could cause that?" she asked.

"Could be fraud," the salesperson said.

She suggested that Sybesma contact a credit bureau. When Sybesma did, she obtained a copy of her credit report, which showed that someone had

opened several credit card accounts in her name and charged \$10,000 worth of items. But how? Her mind immediately began racing through the possibilities. Stolen wallet, stolen mail, a mistake on the report – what could it be? Sybesma blamed herself. How could I have been so stupid as to let this happen to me? she thought.

Her self-blame then gave way to determination. She turned detective and began collecting all the evidence she could find in an effort to catch the thief. The hunt was about to consume her. "It was maddening," recalls Sybesma, a member of the Rotary Club of Fishers, Ind., USA.

### ON THE TRAIL

Sybesma began her investigation by contacting the police in Noblesville, Ind., where she was living at the time. But the police department wasn't prepared to tackle identity theft, a crime that wasn't attracting much attention 12 years ago, and suggested she contact the U.S. Secret Service. The federal agency declined to help

**Out of control** Sybesma, pictured here, was scared after she found out someone had stolen her identity. "All I knew is that very personal information about me was in someone else's hands, and it made me uncomfortable," she says.

PHOTOGRAPHY BY MONIKA LOZINSKA-LEE/RI



*"It sucked the life  
out of me."*

because it considered her situation a minor case, she says. But the Secret Service did recommend contacting the U.S. Postal Inspection Service, because the thief received some credit cards through the mail. That constituted mail fraud.

Sybesma met with Postal Inspector Dan Medrano. Acting on his advice, she told credit bureaus to flag her report with a request for creditors to call her before opening new accounts. But this precaution didn't help. Lenders, such as department stores, would issue credit on the spot without first contacting credit bureaus.

So the thief would go on a spending spree, Sybesma would get charged, and then she'd have to call lenders to explain that she didn't buy the items.

She became familiar with the thief's spending habits over the next couple of months by regularly requesting copies of her credit report. Inevitably, the report would show that new credit card accounts had been fraudulently opened in her name. She would then contact the creditors to get listings of all the charges on each card. For example, someone was using a credit card issued in her name to dine weekly at a steakhouse on the west side of Indianapolis. She stopped at the restaurant to see if she recognized anyone who worked or dined there, but to no avail. She also drove

by a house that the thief had listed as Sybesma's residence on numerous credit card applications, but she didn't recognize any cars out front. Scared, she didn't knock on the door or try to find out who lived there.

In the meantime, Sybesma quit her hotel job and took a position as a travel agent. When she wasn't working, she was spending countless hours on the phone repairing the damage to her identity and trying to track down the thief. She called stores that had issued credit cards in her name, hoping the clerks might remember who made the purchases. She made long-distance calls to credit bureaus to rectify the incorrect information on her credit report. Because the bureaus lacked toll-free phone numbers for their fraud departments at the time, the phone bills mounted, as did her frustration. She also called credit card companies and asked them to send her copies of the thief's fraudulent, handwritten applications.

Every day, Sybesma pored over the credit card applications, looking for clues. She discovered that the thief was changing bits of information about her when applying for credit. First, her address was changed, then her gender. Her name gradually morphed too. Credit card applications listed





Private eye “I am not the kind of person who misses details,” says Sybesma, who spent hours scrutinizing credit card applications in search of the thief.

her as Jamie M., Jamie Michelle, and Jamie Michael. She had the perfect first name for the crime: It was gender neutral, so the thief could be either a man or a woman.

A few months after she'd begun her investigation, Sybesma sat in her living room and spread copies of credit card applications and other paperwork around her. She arranged the documents chronologically, trying to recall where she had been and whom she had met during the previous months. She knew the answer lay somewhere in those papers. If she looked hard enough, she could figure it out. Then she saw a copy of an American Express application. Her address had been crossed out and replaced with a different address. The application also contained her work history, Social Security number and, unlike previous

applications, her checking account number – or at least what looked like her number. When she took a closer look, she noticed a few extra digits at the end.

The thief had mistakenly written a check number after the account number, an easy mistake if the person had hastily copied the information while stealing a quick look at a check, Sybesma thought. After all, both numbers are printed along the bottom edge of every check.

Sybesma still had the canceled check that matched the number; she'd used it to pay for garbage pickup. Realizing that someone must have touched the check while writing down the number, Sybesma put it in a plastic bag and gave it to Medrano to run for fingerprints.

Once prints showed up on the check, they were linked to a clerk at the hotel where she had worked earlier that year. She had handed her employment application to him when she applied for the job. Sybesma figured he made a copy of her application, which included her Social Security number, date of birth, and address. She surmised that he later rifled through her purse in a hotel break room and opened her checkbook to obtain a checking account number, which some credit applications require. Medrano informed her that the man was part of a criminal ring responsible for various identity thefts. After being arrested in

**EXPERIENCE MADE HER WISER**

*Sybesma offers these tips for preventing identity theft:*

- Never share more information than necessary.
- Always create intelligently devised passwords.
- Promptly review your bills and bank statements.
- Routinely check your credit report for suspicious activity.



---

---

connection to Sybesma's case, the man was offered a plea bargain for helping to clear other cases, Medrano said.

#### **NOW AN ADVOCATE**

After the initial elation of finding the culprit, Sybesma became slightly depressed. "I went through a down period, I think from pure exhaustion," she says. "It sucked the life out of me. I had a hard time. I felt violated, and I was spent."

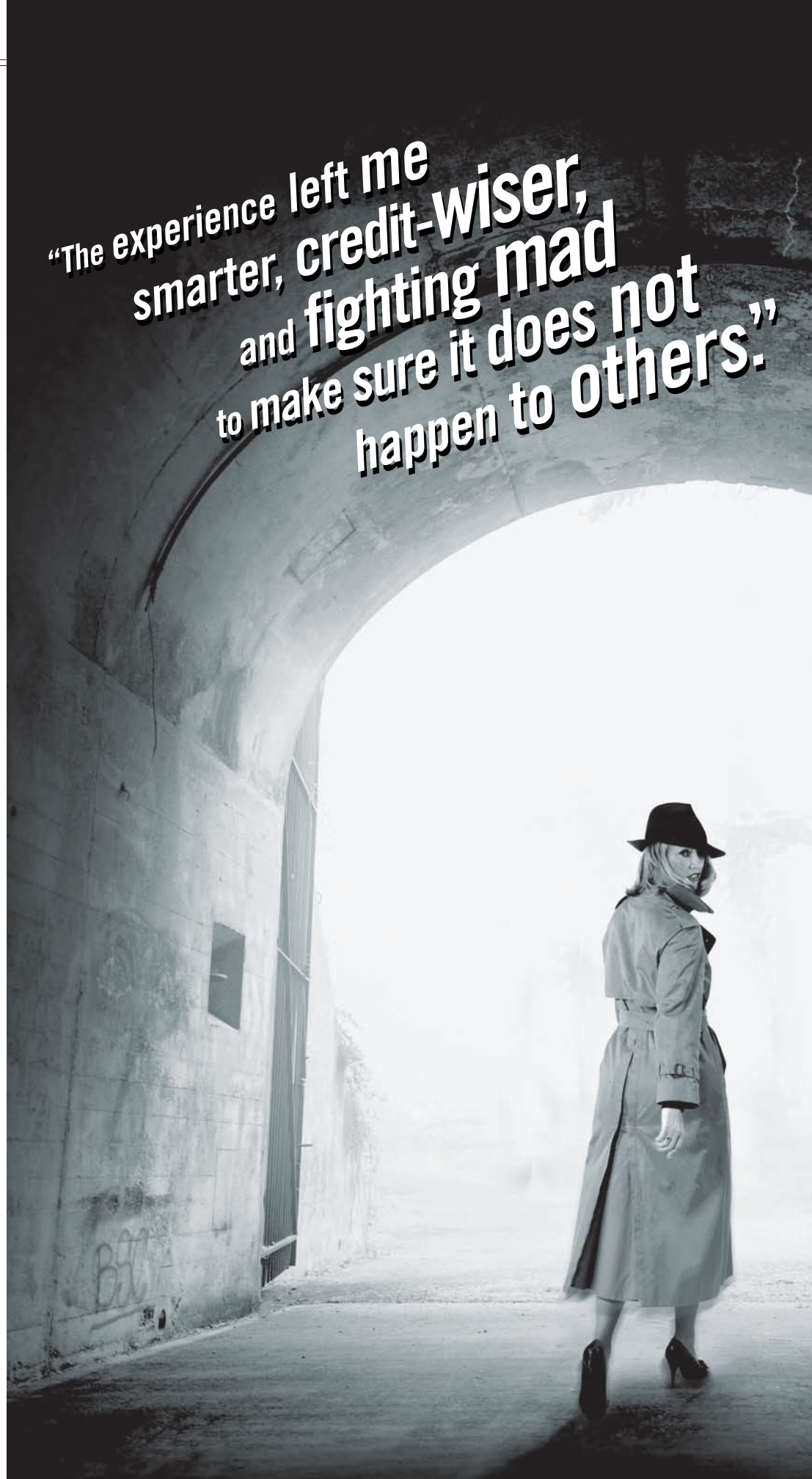
But she bounced back and decided to use her experience to educate people about identity theft. She lobbied her congressional representative to update credit reporting laws and began speaking publicly about identity theft.

In 1999, Sybesma established a consulting agency to help businesses improve their productivity. She now talks to groups and companies about customer service and organizational techniques, and her lineup of topics includes tips for preventing identity theft.

"I am inclined to believe things happen for a reason, and this happened to me so I might teach others how to prevent it," she says. "The experience left me smarter, credit-wiser, and fighting mad to make sure it does not happen to others. As I always say in my presentations, avoiding identity theft is like avoiding germs. You can't avoid it completely, but you can be smart." ■

---

*Dean Rea is an adjunct assistant professor of journalism at the University of Oregon. Additional reporting by Senior Editor Tiffany Woods.*



**"The experience left me smarter, credit-wiser, and fighting mad to make sure it does not happen to others."**



## Get smart

*How to outfox identity thieves and repair the damage they do*

by Rob Hamadi

This wasn't exactly the way John Sileo had wanted to start his day. On the morning of 11 September 2003, a local law enforcement official knocked on the door of his home near Denver and told him he was being investigated for stealing almost \$300,000.

During the next two years, Sileo, a 1992-93 Rotary Foundation Ambassadorial Scholar to New Zealand, spent more than 500 hours and over \$10,000 in legal fees to keep out of jail. He spent days making phone calls and appearing in court, evenings working with lawyers, and weekends feeling depressed. He had little time for his wife and two children. One night before bed, his four-year-old daughter asked him why he didn't tell her bedtime stories anymore. How could he tell her that he was too busy for stories because someone had stolen his identity?

A friend, who was also a rock-climbing buddy and a business partner, had opened a credit card account in Sileo's name and, during the 16 months before the investigator's knock on the door, used it to charge

\$298,567 worth of items. To pay off the bulk of the charges, the friend stole account and routing numbers from the bottom of checks belonging to more than 160 people. Some of the checks were customer payments from the business. Using the Internet, the fiend electronically transferred funds from the checking accounts into the fraudulent credit card account.

The friend was eventually jailed for the crime, and Sileo went on to write a book about identity theft called *Stolen Lives: Identity Theft Prevention Made Simple*. He now gives speeches about identity theft and has talked to Rotary clubs about the topic.

This case shows just how grave identity theft can be. It's enough to make you reluctant to trust anyone, even a friend or co-worker. But, as Sileo says, "there is no need for paranoia if you're educated about how to prevent identity theft."

### WHAT IS IT?

To get educated about the crime, you first need to understand what it is. The U.S. Federal Trade Commission (FTC) defines

Light at the end of the tunnel Sybesma walked away from her ordeal with a determination to help others avoid becoming victims.

identity theft as “fraud that is committed or attempted using a person’s identifying information without authority.” The term *identity theft* is an umbrella label for a wide range of crimes.

Allan E. Jones, director of corporate security for Wood and Huston Bank and a member of the Rotary Club of Marshall, Mo., USA, teaches classes on repairing the damage caused by identity theft. “Ten years ago, when someone tried to use a stolen credit card, we called it fraudulent use of a credit device,” he says. “When someone used a bogus name and Social Security number to open a new account at the electric company [or other service provider], we called it theft of service. And when someone signed your name on a check and presented it as payment, we called it forgery. Today, all these crimes fall under identity theft.”

Knowing this range can help you keep the statistics on identity theft in perspective. A 2003 FTC-sponsored survey estimated that almost 10 million Americans discovered they were

victims of identity theft during the previous year. The U.S. Department of Justice said an estimated 3.6 million American households – about 3 percent of all households in the country – learned they had been victims of identity theft during a six-month period in 2004. And last year, Consumer Sentinel, a database developed and maintained by the FTC that collects fraud reports, received 255,565 complaints of identity theft, accounting for 37 percent of all complaints that year. Credit card fraud was the most common form of identity theft, Consumer Sentinel said.

**HOW DOES IT HAPPEN?**

Although the precise number of identity theft victims may never be known, how identity theft occurs is no mystery. Most identity theft crimes fall into three categories: account takeover, account creation, and wholesale assumption of identity.

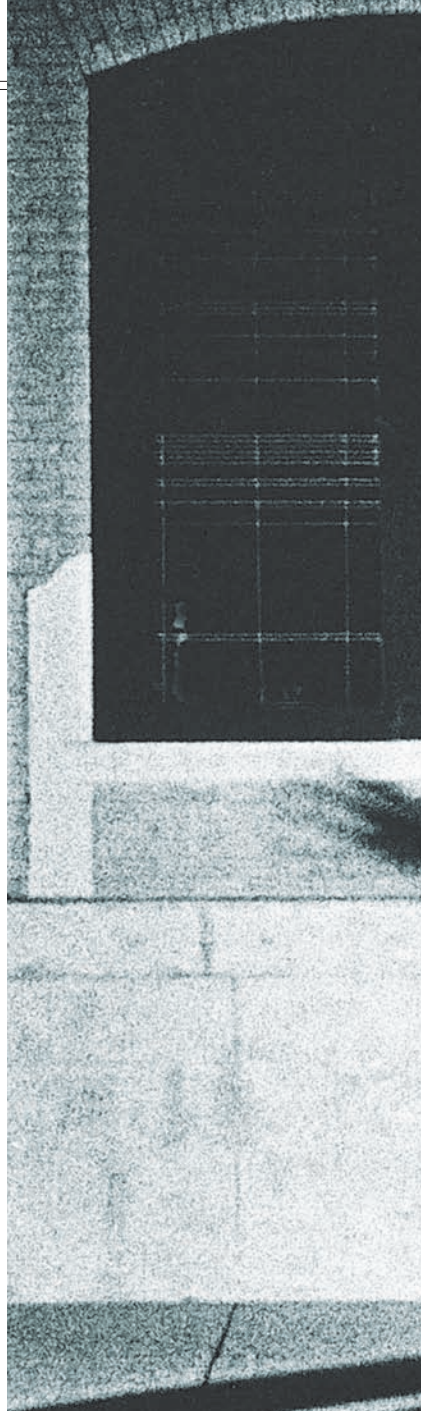
Account takeover is the most common type. The thief simply uses someone’s existing account,

such as a credit or debit card, to make purchases. Fortunately, this form of the crime is also the easiest to spot because the crooks typically follow certain spending patterns, which many banks can detect using specialized software. Patterns that can trigger the detection system include excessive spending abroad and spending in multiple areas at the same time.

Account creation, however, can take longer to recognize. Starting with the most basic information such as a name, date of birth, or Social Security number, a crook opens accounts in someone else’s name. Often, these accounts aren’t spotted until victims check their credit report or, worse, find themselves fielding calls from collection agencies after the thief defaults on the debt.

Jones was a victim of account creation. When he and his wife were applying for their most recent mortgage, he found debts in default on his credit report that were billed to him at an address in the Bronx, a New York borough he’d never visited. “Someone helped himself to my name and Social Security number, then opened a cell phone account, electric utility service, and [leased] an apartment,” he says.

Wholesale assumption of identity reaches much wider, but it’s thankfully the least common of the three categories. In this case, the crook commits the first two types of fraud but goes beyond them by assuming someone’s identity in areas outside a simple credit agreement. Starting with one or more pieces of information, such as a Social Security



number, the thief applies for other official forms of identification, such as a driver’s license or passport. The thief can then go on to get a job, receive benefits, or open accounts. This crime is usually detected only once the victim notices its negative consequences.

Identity thieves use all kinds of strategies to get the information they need to commit these crimes. Some crooks search the trash for documents containing personal

**HOW TO OBTAIN YOUR CREDIT REPORT**

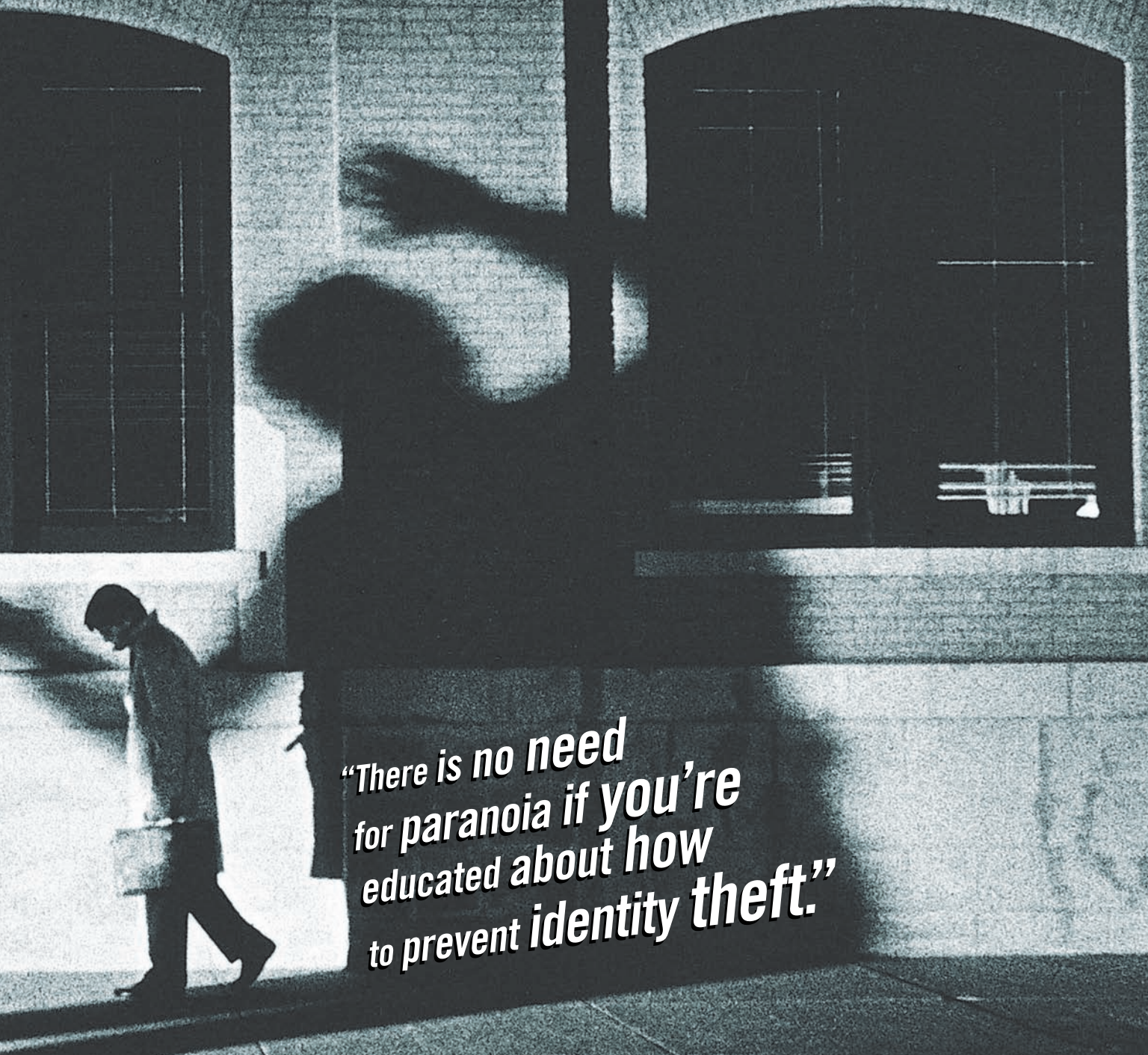
**In the United States**, the three credit-reporting bureaus (Equifax, Experian, and TransUnion) are each required to provide you with a free copy of your credit report annually at your request.

The bureaus have set up a central facility for processing requests. You can order your report by going to [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling 877-322-8228, or by writing to Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281. If you write, enclose a completed request form, available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

One caveat: Look out for crooks operating fraudulent sites to steal data; they often use Web addresses that slightly misspell the name of a legitimate site.

**In Canada**, you can request a free credit report by mail from Equifax. To download a request form, go to [www.equifax.com/EFX\\_Canada](http://www.equifax.com/EFX_Canada), click Consumer Information Centre, then click Your Credit Report. Canadians also can get a free report once a year from TransUnion. Find more information at [www.tuscores.ca/Personal](http://www.tuscores.ca/Personal).





***“There is no need  
for paranoia if you’re  
educated about how  
to prevent identity theft.”***

data, an easy way to turn up information that they can eventually sell or use for fraud. Others employ a skimmer, an electronic device sometimes used maliciously by waiters and clerks to read magnetic stripes on credit cards. The scam works like this: You hand your card to a waiter, who swipes it twice – once for the real transaction and once through a hidden skimmer, which fits in an apron pocket.

The skimmer stores your data, which the thief can later access.

Of course, crooks use other methods as well. Corrupt employees sell customers’ personal information, and tech-savvy hackers crack corporate databases, eavesdrop on cell phone calls, and steal data transmitted over insecure wireless networks. Thieves also tour neighborhoods to take bank statements and preapproved credit card

applications from mailboxes. And don’t forget about online techniques in which crooks send bogus e-mails pretending to be from banks and Web sites like eBay and PayPal.

But the most pernicious form of information gathering may be the pretext call. For example, a crook might call you and purport to be from your credit card company. The thief might say the company caught a person

fraudulently using your account number and needs to verify some information to bring charges against the person.

“Pretext calls are a problem for consumers in general and seniors in particular,” says Rob McKenna, attorney general for Washington state and a member of the Rotary Club of Bellevue. “Crooks target seniors for two reasons: The older generation has a larger share of the nation’s

wealth and, because they're home more, they're more likely to answer the phone." In 2005, McKenna's office teamed up with AARP and the FTC to tackle this crime. As part of the effort, volunteers received training in identity theft prevention and shared the tips they learned with seniors. McKenna also convened Washington's first statewide summit to address identity theft.

**HOW CAN YOU PREVENT IT?**

To reduce the chance that identity theft will happen to you, take these precautions:

- Buy a shredder to destroy receipts, statements, and bills.
- Install antispyware and antivirus software on your computer, and use a firewall.
- Encrypt data transmitted over wireless networks.
- Keep your credit card in sight at restaurants and gas stations.
- Don't divulge your Social Security number, account numbers, or passwords unless you know who you're talking to and how that person will use your information. If someone calls you claiming to be from a bank or any other organization and requests personal information, ask for the person's name and department, then call the company back using a phone number you know is legitimate, like one from the phone book or the back of your credit card. Don't use a number the caller provides.
- Know when your financial statements and bills should arrive in the mail. If they don't turn up, someone may have stolen your mail or changed your address.

- Remove unnecessary information from your wallet. Do you really need to carry your Social Security card?
- Pay with cash when possible.
- Pay bills online so your statements and payments won't be stolen in the mail. Make sure you use a secure connection.
- Install a locking mailbox.
- In the United States and Canada, opt out of offers for pre-approved credit cards by calling 1-888-567-8688.
- Check your credit report.

**WHAT IF YOU BECOME A VICTIM?**

No matter what precautions you take, you may still fall prey to identity theft. What then? Consider these suggestions to start getting your life back:

- Request a current copy of your credit report.
- Ask credit reporting bureaus to place a fraud alert on your report. The alert tells creditors to contact you before opening or altering accounts.
- Close accounts that are opened fraudulently or might have been tampered with. In the United States, the FTC provides an affidavit, available at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), to use when disputing new accounts.
- Report the crime to the police and other appropriate agencies. In the United States, for example, you might contact the Social Security Administration, Internal Revenue Service, Department of Motor Vehicles, Federal Bureau of Investigation, Postal Inspection Service, or Secret Service.
- Keep records of all correspondence as you sort out the situation. Write down dates, the

names of the organizations you call, the names of the people you speak with, and what they say. Follow up conversations in writing. Keep a log of the costs you incur and the time you spend on the case. You may be able to use this information in a claim for damages against the thief.

- Keep copies of all letters or forms that you mail. According to Martha Lucey, a member of the Rotary Club of Fresno, Calif., USA, and an executive vice president at ByDesign Financial Solutions, when you write to credit bureaus or creditors to dispute fraudulent charges, you should include your name, address, Social Security number, date of birth, a statement that you believe you are a victim of identity theft, information about the disputed items, and copies of a police report and the FTC identity theft affidavit. Lucey's company teaches clients to prevent and cope with identity theft.
- Notify the relevant agency and request new documentation if any of your government-issued identification has been lost or stolen.
- File an identity theft complaint with the FTC if you live in the United States. Such complaints help the agency investigate fraud and can lead to legal action. The form is available at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

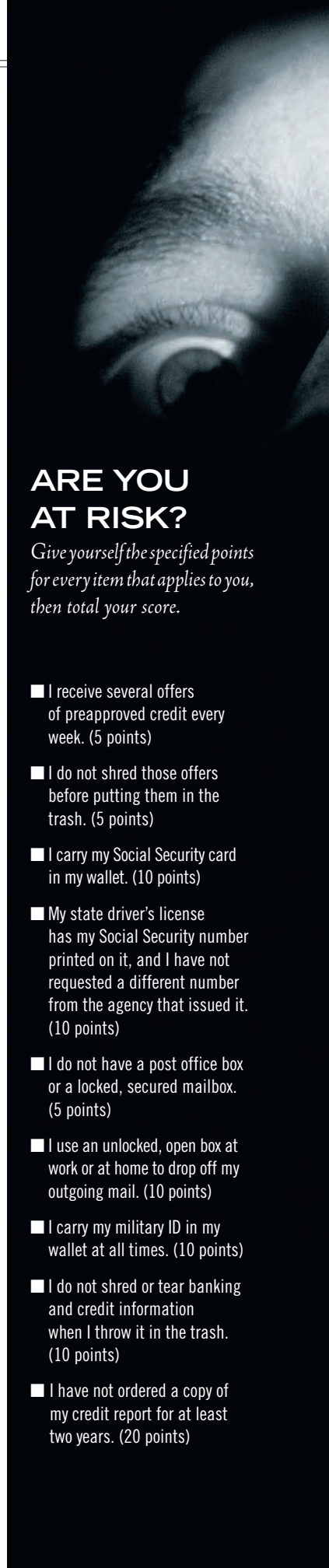
Remember, if you do become a victim, it's not the end of the world. In most cases, the situation can and will be resolved. ■

*Rob Hamadi lives in London and is the author of Identity Theft: What It Is, How to Prevent It, and What to Do If It Happens to You.*

**ARE YOU AT RISK?**

*Give yourself the specified points for every item that applies to you, then total your score.*

- I receive several offers of preapproved credit every week. (5 points)
- I do not shred those offers before putting them in the trash. (5 points)
- I carry my Social Security card in my wallet. (10 points)
- My state driver's license has my Social Security number printed on it, and I have not requested a different number from the agency that issued it. (10 points)
- I do not have a post office box or a locked, secured mailbox. (5 points)
- I use an unlocked, open box at work or at home to drop off my outgoing mail. (10 points)
- I carry my military ID in my wallet at all times. (10 points)
- I do not shred or tear banking and credit information when I throw it in the trash. (10 points)
- I have not ordered a copy of my credit report for at least two years. (20 points)





## Too much information

*There are just some things others don't need to know about your clients, consumers, or employees*

by Chris McMahon

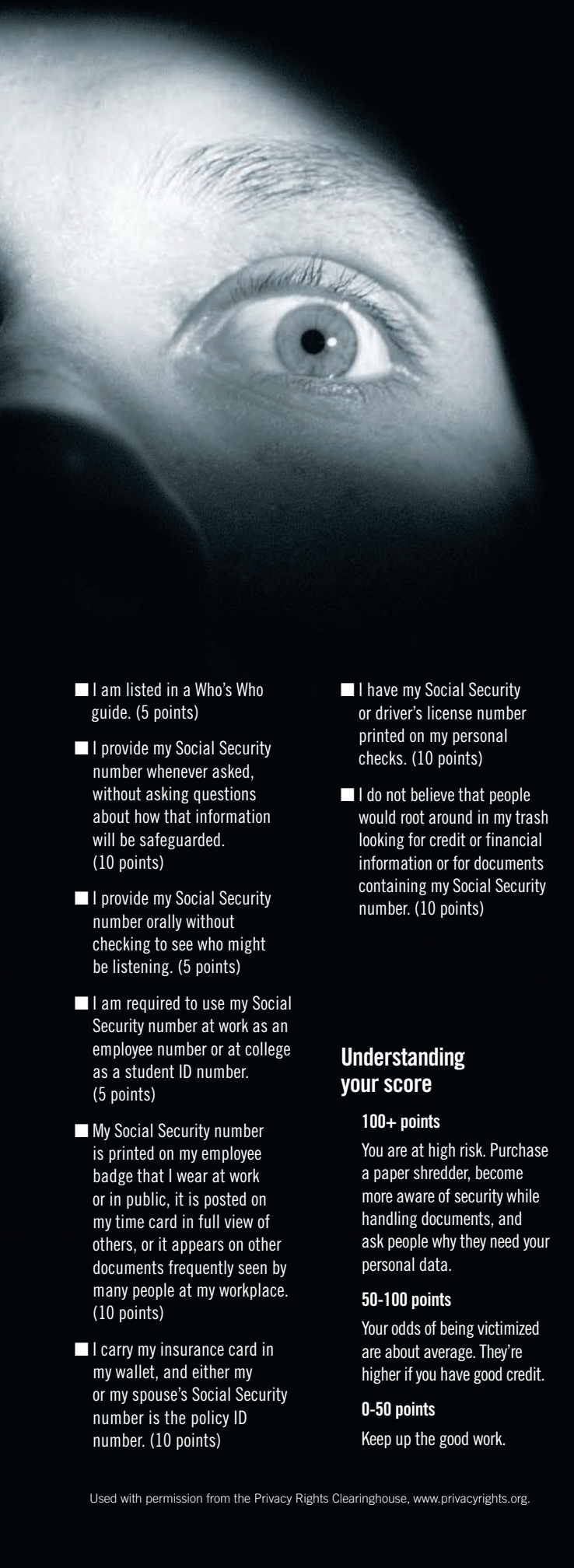
September 27, 2004, is a day ChoicePoint Inc. won't forget. That's when the company, which sells consumer data, discovered what it calls "evidence of suspicious activity" by a few of its customers. An investigation later found that these customers were con artists pretending to be affiliated with businesses so they could purchase data from ChoicePoint. They bought information about 163,000 consumers, including individuals' names, addresses, driver's license numbers, and Social Security numbers.

The U.S. Federal Trade Commission (FTC) looked into the matter and said at least 800 cases of identity theft resulted from the incidents, but ChoicePoint says the number is lower. The FTC also alleged that ChoicePoint failed to implement reasonable procedures for verifying the identities of prospective clients who wanted to access company databases.

The breach hit ChoicePoint in the pocketbook. The company agreed to pay the

FTC \$10 million – the largest civil penalty in the commission's history – to settle charges that its security and record-handling procedures violated federal laws and consumer privacy rights. The company also agreed to put \$5 million into an FTC-administered fund to compensate consumers affected by the fraud. ChoicePoint, which admitted to no wrongdoing as part of the settlement, continues to shell out money for its defense. In the first quarter of this year, it racked up more than \$800,000 in legal fees related to the situation. The company said in April that it expects this year's legal costs, not including potential settlements, to reach up to \$4 million.

ChoicePoint's costly lesson illustrates how crucial it is for businesses to protect the personal information they handle, whether it belongs to consumers, clients, or employees. If you're like a lot of working Rotarians, you've probably got health records on patients, files on employees, or financial information on clients. And if you don't safeguard this



- I am listed in a Who's Who guide. (5 points)
- I provide my Social Security number whenever asked, without asking questions about how that information will be safeguarded. (10 points)
- I provide my Social Security number orally without checking to see who might be listening. (5 points)
- I am required to use my Social Security number at work as an employee number or at college as a student ID number. (5 points)
- My Social Security number is printed on my employee badge that I wear at work or in public, it is posted on my time card in full view of others, or it appears on other documents frequently seen by many people at my workplace. (10 points)
- I carry my insurance card in my wallet, and either my or my spouse's Social Security number is the policy ID number. (10 points)

- I have my Social Security or driver's license number printed on my personal checks. (10 points)
- I do not believe that people would root around in my trash looking for credit or financial information or for documents containing my Social Security number. (10 points)

### Understanding your score

#### 100+ points

You are at high risk. Purchase a paper shredder, become more aware of security while handling documents, and ask people why they need your personal data.

#### 50-100 points

Your odds of being victimized are about average. They're higher if you have good credit.

#### 0-50 points

Keep up the good work.

## INFORMATION ON THE LOOSE

*Here's a rundown of data breaches that exposed personal information to potential misuse:*

### BANK OF AMERICA

Computer backup tapes were lost en route to a data center in December 2004. Addresses and Social Security numbers of federal employees were on the tapes. **Exposed: 1.2 million**

### DSW

Hackers stole transaction data from more than 100 of this shoe retailer's stores primarily between November 2004 and February 2005. Checking account, driver's license, and credit and debit card numbers were compromised, along with customers' names. **Exposed: 1.5 million**

### CITIFINANCIAL

A box of computer tapes containing information about CitiFinancial's customers was lost during a routine shipment to a credit bureau, the company announced in June 2005. The tapes contained names, Social Security numbers, and account numbers. **Exposed: 3.9 million**

### THE BOSTON GLOBE AND WORCESTER TELEGRAM AND GAZETTE

Credit and bank card numbers from both newspapers' subscribers were accidentally distributed along with bundles of *Telegram and Gazette* papers in January. The data was printed on paper used to wrap the newspaper bundles for distribution. **Exposed: Up to 240,000**

### AMERIPRISE FINANCIAL

A company-owned laptop was stolen from an employee's locked car, the firm said in January. Its files contained clients' names and account numbers as well as the names and Social Security numbers of current and former financial advisers. **Exposed: 158,000**

### PEOPLE'S BANK

A computer tape containing customer and employee data was lost while being shipped to the TransUnion credit reporting bureau, the bank said in January. The tape contained names, addresses, Social Security numbers, and checking account numbers. **Exposed: 90,000**

— RAMAH KUDAIMI

information, you may find yourself in trouble with the law. Even if laws don't regulate your data, you are ethically obligated to make sure lives aren't turned upside down because of carelessness on your part.

Somesayexperienceisthebest teacher,so to help you protect sensitive information at work, we compiled the following examples of data breaches. Then we asked the experts – some of them Rotarians – how to prevent information in such scenarios from falling into the wrong hands.

## DESTROY IT OR LOCK IT UP

### ►WHAT CAN HAPPEN

It's an identity thief's dream: heaps of discarded personal documents containing names, addresses, Social Security numbers, and medical records. That's exactly what a TV news crew found in March when it reported that the Los Angeles County Department of Public Social Services had left boxes of sensitive files beside a recycling bin in the parking garage outside an office. In April, a department spokesperson said no identity thefts had been tied to the incident. Nevertheless, the agency alerted 94,000 people that their information may have been compromised.

### ►WHAT YOU CAN DO

1. Never leave sensitive information where unauthorized people could see or steal it. Don't leave documents in printers, fax machines, conference rooms, or trash containers.
2. Educate employees so they understand the value and sensitivity of the information they handle. "Make sure they know what is expected" and that they

manage the information appropriately, says Jack McCoy, vice president of security at Discover Financial Services and a former employee of the U.S. Federal Bureau of Investigation.

3. Destroy documents. Information has a shelf life and can become a legal liability, says Tom W. Brown, of the Rotary Club of San Luis Obispo, Calif., USA. As president of DocuTeam, Brown makes his living by shredding, storing, and digitally archiving information for businesses. Crosscut shredders cost as little as \$25, so buy several and plug them in near printers and fax machines. Larger companies should consider hiring professionals to destroy documents, Brown says. Specialists can install locked drop boxes in offices, witness on-site destruction of documents, or offer certified off-site destruction. "It all comes down to this: Protect it while you have it. Get rid of it when you can. And get rid of it the right way," Brown says.

## STOP HACKERS

### ►WHAT CAN HAPPEN

The Employees' Retirement System of Georgia knows all about hacking. In February, someone got into its database, which held account and Social Security numbers for state employees and pensioners.

### ►WHAT YOU CAN DO

1. Be careful where you store information. "If a business owner is storing sensitive data on his customers, he shouldn't store that information on a computer used to access the Internet," says Allan E. Jones, director of corporate security for Wood and Huston Bank and a member of the Rotary

Club of Marshall, Mo., USA. "If that computer isn't professionally configured, you're just looking for trouble."

2. Install firewall, antivirus, and antispyware software to prevent your computers from being hijacked through the Internet and to keep them free of malicious programs that can destroy information or allow unauthorized users to access your data. Larger companies should consider intrusion detection systems or a secure virtual private network (an encrypted network that connects users over the Internet).

3. Secure your transactions. If you're accepting credit card numbers online, use Secure Socket Layer encryption, which was developed for transmitting private information. You can tell if a Web page is using this tool because its Web address will start with *https* instead of *http*.

## GUARD LAPTOPS

### ►WHAT CAN HAPPEN

A laptop was stolen in January from the locked car of an Ernst and Young employee. The laptop contained the names, birth dates, Social Security numbers, and electronic tax forms for tens of thousands of employees at Nokia, Sun Microsystems, Cisco Systems, IBM, BP, and other organizations within the firm's clientele. In April, a spokesperson for Ernst and Young said the laptop was password protected and that the theft had not resulted in fraud.

### ►WHAT YOU CAN DO

1. Don't take laptops containing personal information outside the office. If you do, encrypt sensitive data. "We simply don't allow bank-owned laptops with

customer data off the premises,” Jones says. He adds that if you must put customers’ information on a laptop, you should encrypt it – that is, convert it to a coded format that requires a separately stored key. That way, if the laptop were lost or stolen and the login password cracked, the data would still be unintelligible without the key.

2. Make sure it’s safe. “Never leave your hotel room without locking the laptop,” says Darity Wesley, a member of the Rotary Club of La Jolla Golden Triangle, Calif., USA, and chief executive officer and legal counsel for Privacy Solutions Inc., a privacy and information security consulting company. Put your laptop in the hotel safe, or use a cable lock. Never leave it visible in your car.

**SCREEN EMPLOYEES**

➤ **WHAT CAN HAPPEN**

An employee for the City of San Diego was sentenced in March to two years in prison after pleading guilty to two counts of identity theft. She was accused of using her position as a city worker to access the local water billing system and obtain customers’ personal information. The city now blocks employees from viewing Social Security and driver’s license numbers and has issued orders to modernize its 20-year-old water billing system.

➤ **WHAT YOU CAN DO**

1. Check employees’ backgrounds. McCoy recommends searching academic, public, and courthouse records for arrests and criminal convictions, especially for people who will have access to sensitive information,

such as accountants and human resources personnel. You also can purchase background checks from private investigation firms and online vendors. Fingerprinting employees and searching for their names in criminal databases might be warranted during the hiring process or when a crime occurs in the workplace, McCoy says.

2. Consider what information employees can view, and make sure employees who leave the company don’t take data with them. Access to sensitive information, such as medical, financial, and personal data, should be on a need-to-know basis.

3. Scrutinize software vendors, consultants, and others who can access your systems and records. “You should be doing some due diligence on that vendor

and communicating expectations for access, storage, and encryption of data,” McCoy says. Arrange for data to be returned or destroyed, and specify when and how that process should happen.

When data breaches occur, McCoy advises: “If I could stress one thing, it would be that you [should] act quickly and decisively. Bad news only gets worse if you wait. It only creates more distrust. If you don’t build customer trust, you can’t build customer loyalty, [which] is crucial if you want to survive.” ■

*Chris McMahon lives in Evanston, Ill., USA, and is an associate editor for Futures magazine. He is the proud owner of a crosscut shredder.*

**KNOW THE LAW**

*Depending on your profession, you might need to study up on the regulations for handling personal information. Here are several:*

- If you work for a consumer reporting agency, you should know the U.S. **Fair Credit Reporting Act**, which says employees of consumer reporting agencies will be fined or imprisoned if they knowingly and willfully provide information about individuals from agency files to an unauthorized person.
- If you work for a health plan, health care clearinghouse, or health care provider, you may need to know about the **HIPAA Privacy Rule**. Issued by the U.S. Department of Health and Human Services, this rule establishes national standards for protecting certain health information. You’ll also want to check out the **Security Rule**, which provides regulations for safeguarding electronic health care information.
- If you’re handling consumer reports, including information related to credit, employment background, insurance claims, and tenant history, learn the FTC’s **Disposal Rule**. This rule went into effect 1 June 2005 and requires businesses to properly dispose of consumer reports through shredding, burning, or other approved methods.
- If your business accepts credit and debit card payments, you should know the U.S. **Fair and Accurate Credit Transactions Act**, which says electronically printed receipts can list no more than the last five digits of a card number, although the enactment date varies according to when businesses installed their credit card scanners.
- If you work in Canada, you may want to study the **Personal Information Protection and Electronic Documents Act**, which specifies guidelines for private-sector organizations that collect, use, and disclose clients’ personal information during commercial activity.