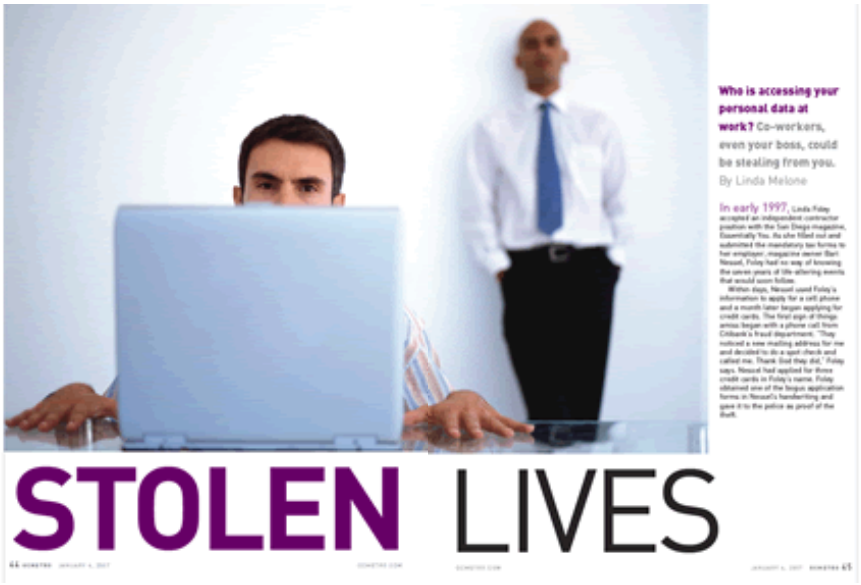
OCMETRO BUSINESS

FEATURE STORY
JANUARY 4, 2007



STOLEN LIVES

Who is accessing your personal data at work? Co-workers, even your boss, could be stealing from you.

By Linda Melone

ALSO: WHERE TO GO FOR HELP | HOW TO PROTECT YOURSELF

In early 1997, Linda Foley accepted an independent contractor position with the San Diego magazine, Essentially You. As she filled out and submitted the mandatory tax forms to her employer, magazine owner Bari Nessel, Foley had no way of knowing the seven years of life-altering events that would soon follow.

Within days, Nessel used Foley's information to apply for a cell phone and a month later began applying for credit cards. The first sign of things amiss began with a phone call from Citibank's fraud department. "They noticed a new mailing address for me and decided to do a spot check and called me. Thank God they did," Foley says. Nessel had applied for three credit cards in Foley's name. Foley obtained one of the bogus application forms in Nessel's handwriting and gave it to the police as proof of the theft.

A search uncovered other victims of Nessel's and resulted in 31 criminal counts, mostly check fraud and one identity theft charge: Foley's. It took until 1999 for a judge to sentence Nessel to five years probation and 240 days of jail time, which would be set aside if she abided by the terms of

probation. She violated probation and was sentenced to three months in jail, after which, she was released. She continued to violate her probations and in 2004 a judge sentenced her to confinement for more than three years.

To help others in the same quandary, Foley founded the San Diego-based Identity Theft Resource Center (ITRC) in 1999, a national nonprofit victim services, advocacy and consumer education program in response to the epidemic rise in identity theft. Her personal experience enables her to understand the complexities of the crime and to help other victims piece their lives back together.

Workplace is fertile ground for thieves

Last year, approximately 10 million people in the U.S. were identity theft victims, and as many as one in 10 have been hit by the crime in recent years. Identity theft costs employers hundreds of thousands, to millions of dollars and has replaced shrinkage (theft) as the biggest cost to employers after payroll and healthcare.

Armed with a Social Security number and birth date, an identity thief can open new credit card accounts or take over existing accounts, apply for loans, rent an apartment, establish services with utility companies, write fraudulent checks, steal money from bank accounts and obtain employment using the victim's name.

The ease of obtaining information in a work environment contributes to the epidemic growth of workplace identity theft. Thieves will sift through business dumpsters in search of unshredded documents containing Social Security numbers and other personal data.

"Actually, you're just as vulnerable at work as you are at home or out of the house. The workplace is simply one place where identity theft is occurring," says Tom Lawson, founder of APSCREEN, an Orange County applicant screening company.

Employees may gain access to co-workers' personnel files or access credit reporting databases (commonly available in auto dealerships, realtors' offices, banks and other businesses that approve loans).
And alarmingly, as in Foley's case, identities also are stolen by business owners. In a recent case, Terrence Chalk, 44, a well-respected Westchester, N.Y. businessman and his 35-year old nephew were charged with identity theft for allegedly using an employees' personal information to get more than $1 million in bank loans and credit card charges between 2001 and 2006. Chalk is accused of falsely listing his 50 employees as owners and officers of his companies, leaving them on the hook for paying off the notes.

"Although there are cases where employers are the thieves, usually it's employees stealing from other employees," Foley says. "Identity theft is a crime of opportunity." In fact, employee theft and fraud cost U.S. retail businesses more than $50 billion per year and it is responsible for 30% of small-business failures, according to the U.S. Department of Commerce,

which reports embezzlement losses that exceed $4 billion each year. Sadly, relatives and friends – the least-likely suspects – may be the guilty ones. “About two-thirds of us do not know who the thief is, but of those who do, 14% of those are our own relatives,” Foley says.

Do you know your co-workers?

Although a company may implement security policies such as password protection, if employees do not follow or are unaware of them, the policies may as well not exist. Linda Foley tells of a dental office that got into trouble when the office stopped shredding confidential documents because people complained about the noise of the shredder. “Not everyone was trained as to the importance of doing this for security reasons,” Foley said.

“Protecting your identity at work is a matter of personal record management and being cognizant of your information,” Tom Lawson notes. “Be mindful of what you carry with you. Most people carry too much stuff, especially women. Keep your driver’s license with you and one or two credit cards. That’s all you need.” And use common sense. Don’t leave the company laptop in an unlocked car or unattended on a desk. And keep in mind that workplace theft serves purposes other than stealing your identity. “Sometimes people just want to get ahold of another person’s files to snoop or get information they can use against that person.”

Lawson, a 26-year veteran in the identity theft field, says it’s a myth that workplace identity thieves seek out information on job applications. “Background information is usually in a file that’s very protected. They’re more likely to steal from employee benefits files and it’s usually a team of professionals working together, not an individual. Identity theft is a highly sophisticated crime.”

Most cases of identity theft via computer hacking occur when an employee unknowingly opens and downloads a file with a Trojan horse, according to Steve Havert, president and owner of Expetec, a computer repair and IT service company. “Once the Trojan horse is downloaded, it tracks every key stroke the employee makes and sends it to the hacker’s server,” Havert says. “They mine that data for information like strings of numbers of credit cards. The hackers let these programs do the work for them and send it to them. They don’t have to be online themselves.” Havert notes that these are typically not the professional hackers that large companies need to worry about. “Professional computer hackers do that stuff for a living and are more likely to hack into bank data bases or large healthcare facilities. It’s not something anyone can just do.”

Havert notes that people typically have their identities stolen via computers by one of two ways: by losing their laptops (or having them stolen) or throwing out a computer without wiping the hard drive clean before doing so. He suggests taking basic precautions like having your computer password protected and not telling anyone what it is, for example. And consider having a professional clean out your hard drive before tossing your

computer if you don't know how to do it yourself.

In addition, he cautions, "Be careful of where you go on the Internet. One client opened a virus when she was performing a search for toner cartridges. The cartridges were cheap, but it is likely the company wasn't making money selling toner cartridges, but by selling her personal information." Look for a picture of a padlock at the bottom of your screen when ordering online to be assured your personal information is encrypted and not there for the world to see.

Worst-case scenarios

When your neighbor hacks into your home computer and steals your iTunes, it's one thing. But when professional hackers find a way into customer accounts at online brokerage firms, like the recent ETrade incident, millions of dollars may be lost: $18 million, in this case. Thieves used customers' money to drive up the prices of little-traded stocks and then sold shares they bought earlier at a profit.

"People who steal your information by getting ahold of your bag are amateurs. The pros that are making a lot of money at it are using electronic methodology to do it," says Ron Williams, founder of Talon Executive Services, Inc. and a retired Secret Service Agent. "It's usually a group, and they're very sophisticated in their approach." Williams credits the Nigerians with "perfecting" identity theft back in the '80s. "They would come over here as students and take one of three jobs: bank teller, taxi driver [for mobility] or janitor, which would give them unfettered access to steal data."

Williams cites a recent incident at a San Diego restaurant where waiters "skimmed" or collected customers' information from their credit cards by running them through a skimmer, a device attached to the waiters' belts that gathers information. "They would collect the information and send it to Tijuana. It was done out in the open and customers would never know it happened."

To catch a thief

Although California prosecutors are pushing for harsher new laws, identity theft wasn't declared a federal crime until 1998, under "The Identity theft and Assumption Deterrence Act of 1998." Another new law passed in 2003, SB 1386, mandates that companies and organizations must protect personal information against possible identity theft and, if an incident occurs that compromises personal information, the company has a fiduciary responsibility to notify all of its customers. This creates huge losses for banks like Wells Fargo, which was recently hit for the fourth time in less than three years. Customer names, Social Security numbers and addresses had been stolen, and many people withdrew their money as a result.

Unfortunately for its victims, identity theft remains a profitable crime, and the majority of thieves are not caught. "It's like trying to catch a wisp of a cloud," says Linda Foley. "By the time you realize your identity's been stolen, the thief is long gone. How do you find that one website or one credit card [that fueled the theft]? You're on a lot of databases." She notes that it's often only when a thief gets greedy that they're able to trace the crime back to its source. "If someone is determined to steal your identity, they probably will."

Emotional impact

The financial damage to an individual is most often minimal and sometimes pales in comparison to the emotional impact of identity theft. Victims of identity theft usually don't discover the theft for an average of three months. It's often devastating to the victim when they realize someone has gone on spending sprees, ruined their credit and even committed crimes in their name. The embarrassment and feelings of helplessness can be life altering.

"Emotionally, I am a changed person. I don't trust like I used to," says Foley. "She [Nessel] was my employer, and I was not going to give one more person my Social Security number until I was hired. My refusal to put a SSN on a job application cost me many interviews. I've logged more than 300 hours clearing my name and spending time in court." **OCM**

Linda Melone is a writer and speaker. You can reach her at http://www.lifebeatfitness.com/ or at 949.713.0403.

Back to top

WHERE TO GO FOR HELP:

Identity Theft Center:
idtheftcenter.com

Background checking:
apscreen.com

Computer security:
expetecsoc.com

Business security:
talonexec.com

Identity theft expert Robert Siciliano:
realtysecurity.com

Credit Reporting Agency
Contact Information:
TransUnion: tuc.com

To report fraud: 800.680.7289

Experian: experian.com

To report fraud: 888.397.3742

Equifax: http://www.equifax.com/cs/Satellite?pagename=Home

To report fraud: 800.525.6285

Back to top

HOW TO PROTECT YOURSELF AT WORK

"Seventy percent of all identity theft is committed by those who have access to the data," says Robert Siciliano, identity theft expert and author of "The Safety Minute."

"A secretary is making phone calls while sitting at someone else's desk; she sees a folder with information on clients and makes copies of that information and passes it on to people who then open credit lines, buy cars, etc. It's that simple."

Use common sense to lessen the majority of identity theft opportunities: Don't leave personal belongings or proprietary information unattended.

Privacyrights.org notes that your employer should have the following in place to protect you.

• Conducts a criminal or civil background check before hiring employees

who will have access to personal identifying information, and screens cleaning services, temp services and contractors

• Wipes electronic files, destroys computer diskettes and CD-ROMs and properly removes any data from computers before disposal

• Uses alternate ID numbers instead of Social Security numbers (SSN)

• Requires its health insurance providers to use an alternate number rather than a SSN

• Has trained staff about security procedures when sending sensitive personal data by fax, email or telephone

• Uses photo IDs of employees

• Keeps all personal data about employees and customers in locked cabinets

• Has installed encryption and other data safeguards for workplace mobile computers, such as laptops and PDAs , that contain files with sensitive personal data

• Has a policy of never selling or sharing data about employees or customers

• Does not print full SSNs on paychecks, parking permits, staff badges, time sheets, training program rosters or other work-related paperwork

Visit privacyrights.org for complete list OCM

Linda Melone is a writer and speaker. You can reach her at http://www.lifebeatfitness.com/ or at 949.713.0403.

Back to top