Identity theft easy; repairing its harm nearly impossible

03/06/05

By GETAHN WARD
Staff Writer

Harpeth Hall math teacher Elizabeth Stelling was at home making dinner for her children when police showed up with warrants for her arrest.

So began an ordeal that she said included a jail stint, an indictment by a grand jury and the loss of her teaching job at the all-girls private prep school in Nashville.

It was 14 months before Stelling's name was cleared.

Her mistake?

She lost an organizer containing her checkbook, driver's license and credit cards while at a support-group meeting in a church.

The organizer landed in the hands of thieves. And Stelling became a victim of identity theft, an increasingly worrisome crime ensnaring more Americans in complicated cases in which someone uses their name and personal information to steal money or fraudulently open accounts.

In Tennessee alone, 3,246 cases of identity theft were reported last year, representing complaints from 55 of every 100,000 state residents, according to the Federal Trade Commission's Identity Theft Data Clearinghouse. That was up 17% from 2003, when 47.6 of every 100,000 residents filed such complaints.

Overall, 9.3 million American adults became victims of identity fraud last year, according to a recent survey by the Better Business Bureau and Pleasanton, Calif.-based Javelin Strategy & Research. Nationwide, identity fraud cost $52.6 billion last year, the survey estimated.

Stelling's experience reflects challenges victims face, including the eerie uncertainty about when the crime is really over.

Her experience also shows how thieves have become more crafty. They're combining technology, such as computers that print bogus checks, with low-tech foraging through garbage for information. Those techniques — and large-scale privacy breaches such as the one recently at information-services company ChoicePoint Inc. that gave thieves access to personal information on 145,000 U.S. residents — are putting more people at risk.

"I kept thinking this could be my grandmother sitting in this jail cell, this police car — that this could happen to anybody," said Stelling, 36, recalling her experience.

Stelling was arrested after thieves went to Regions Bank and cashed bogus checks made up in her name. The bank went to the police and filed a criminal complaint. Stelling last week filed a

lawsuit against the bank seeking damages for mental anguish, humiliation and embarrassment she said she suffered.

On average, respondents to the BBB/Javelin survey said it took 28 hours last year to resolve identity-theft crime, down 15% from 33 hours in 2003. Actions by financial institutions such as setting up an industrywide assistance center and in-house identity theft resolution teams are making it quicker for people to resolve identity theft, said Don Phan, an analyst at Javelin and co-author of the survey report.

But, he acknowledges, the crime could continue long after that.

Dressed like Laura Ingalls

After realizing her organizer was missing, Stelling did what most people would do.

She called her bank, AmSouth, a move that prevented a woman who went by the name Donna Summers from cashing one of her checks. Perpetrators also bought items with other checks, but Stelling avoided those payments by informing the merchants that she was a victim of identity theft.

But that was not the end of the matter. In early 2003, at least four bogus checks for $4,380 were drawn on a mortgage company, made payable to Stelling's name, and cashed by thieves at offices of Regions Bank in Davidson and Sumner counties. In her lawsuit, Stelling claims that Regions did not verify the person cashing the check closely enough, via video recordings or checking her background.

Regions spokeswoman Kristi Lamont Ellis declined to comment.

On Oct. 2, 2003, Stelling said police arrived at her home.

Later, she spent hours in a Nashville jail cell with as many as 10 other women.

"Women in the cell called me Laura Ingalls because of the way I was dressed," she said, referring to the character from *Little House on The Prairie*. "They wanted to know what happened. After I told them, they thought it was funny I was the only one there innocent."

Weeks later the charges against her in Sumner County were dismissed, but Regions continued to pursue the matter in Davidson County for more than a year, said David Raybin, Stelling's Nashville attorney.

"It was during that time that she lost her job at the school (Harpeth Hall). That's where the harm came about," Raybin said.

Stelling said Harpeth Hall officials initially were supportive, but that changed after a grand jury indicted her with a co-defendant. Headmistress Ann Teaff called the charges "very serious" in

explaining the move to let her go in April, Stelling said. Teaff said that Harpeth Hall doesn't comment on employment-related actions.

It wasn't until Dec. 2 that criminal charges against Stelling were dropped. E-mails she'd sent to her boyfriend that were retrieved from Harpeth Hall's e-mail server provided proof that Stelling was at the school when the checks were cashed at Regions by the thieves.

"You could say love saved the day," Stelling said, adding, however, that the felony arrest prevented her from finding another job as a schoolteacher.

Stelling said she makes a living installing tiles on walls. Overall, the ordeal cost Stelling $6,500 in attorney's fees and lost wages from missing work to attend to the matter in court, she said.

Her suit seeks $900,000 punitive and compensatory damages combined, reimbursement of legal costs and a jury trial.

'Getting innovative?'

Before her experience with identity theft, Stelling said she thought the crime was only about stealing and using someone's credit card. But the fact that her name was printed on bogus checks and her identity used by more than one person changed that view.

Identity fraud can take different forms, authorities say. There's the perpetrator who looks over someone's shoulder in the grocery line to read a credit card number and enter it into a cell phone while pretending to be on a call. There's the waitress who, after taking someone's credit card to collect payments, uses a scanner the size of a pen to read their card number for forwarding to identity thieves.

Some thieves also are showing up at workplaces on pay day, offering an employee $500 for a $350 paycheck, then using that paycheck to make counterfeit checks charged to the company and cashed by acquaintances of the perpetrators at bank branches.

Gallatin resident Ron DeBerry saw it all before retiring in January as liability risk management executive with Bank of America. "I don't think our problem here is as bad as it is in some parts of the country," he said, citing Southern California, Florida and Texas as the worst areas. "It doesn't mean we don't have a problem."

One advanced method that perpetrators use is to put "skimming" devices on an ATM that reads information off the magnetic stripe on a cash card and transmits it to accomplices. A camera disguised and mounted on the ATM also is used to record the potential victim entering his or her PIN numbers. Perpetrators also can send a potential victim an e-mail that when opened embeds "spyware" that captures keystrokes and recalls information on online purchases and Web sites, DeBerry said.

While greater use of computers creates more opportunities for identity thieves, 68% of incidents result from offline factors such as one's wallet or checkbook being stolen or lost, according to the

BBB/Javelin survey. The identity of key perpetrators also might surprise you. Half of respondents to the survey who knew the perpetrator said it was a relative or friend, neighbor or an in-house employee.

'The real Mr. Tim?'

A certainty about identity theft is the frustration it causes.

WSMV-Channel 4 TV meteorologist Tim Ross has had his own battle with identity theft over the past year. He said he has tried to no avail to get law-enforcement authorities to apprehend a Florida man who assumed his identity.

It began when Ross was notified by a fraud investigator at the former Chase Manhattan Bank that someone had tried to withdraw money from the bank with credit cards obtained in his name.

Ross later discovered the Opalaka, Fla., man not only obtained up to $30,000 of credit but also signed up for service from utility companies and tried to buy a car using Ross' identity.

In conversations with the investigator, the man insisted that he was the real deal and even knew the names of Ross' wife and children and details related to his work and car payments.

Ross has been able to locate the man's address, and surveillance video exists that shows a Hispanic man trying to obtain a credit card using Ross' identity. But police in Opalaka said they won't send investigators.

The U.S. Secret Service is investigating the matter, Ross said, adding the perpetrator also is suspected of stealing other people's identity.

"That really opened my eyes to the problem," Ross said about identity theft. "They know where the person is, heard him on the phone, investigators know where he is and still can't get to him."

Fortunately, Ross said, he hasn't lost any money because he put a hold on his credit by contacting the major credit-reporting agencies. The action put an alert on his credit, but it's also made it difficult to get credit. He now uses his home equity line for borrowing.

The experience also has brought some changes to Ross' lifestyle.

"I look over my shoulder right now," he said, adding he suspects his identity was stolen through a mortgage company in Oklahoma where he lived before relocating to Middle Tennessee.

"I'm unwilling to talk on the phone to businesses. When leaving in the morning, I'm more aware of my surroundings — always watching around me to see if someone is looking. I'm just a little paranoid. "

Protect yourself with vigilance on records, prompt reports of loss

When Vanderbilt University graduate student Heather M. Hair discovered her car had been broken into last summer, her first step was to call the three major credit bureaus to put an alert on her credit.

With the items stolen including checks, bank statements, and other documents, Hair also called her bank to close her accounts.

Experts said such prompt action can go a long way in helping to prevent damage after someone's personal information has been stolen. The fraud alert meant that the credit-reporting agencies — Equifax, Experian and Trans Union — would call Hair to verify if someone sought to obtain credit such as a loan using her identity. It's initially effective 90 days but may be extended for seven years.

Here are other steps consumers can take to protect themselves:

• **Check credit reports:** Kathleen Calligan, chief executive of the Better Business Bureau of Middle Tennessee, obtains a copy of her credit report twice a year — when daylight saving time starts and ends — and reviews it for accuracies. "To me paying that little bit of money is insignificant compared to what it can cost me if I was a victim of identity theft," Calligan said. Under the Fair and Accurate Credit Transactions Act of 2004, the three national credit bureaus are required to provide you with one free copy of your credit report each year. For Tennesseeans, that begins on June 1.

• **Improve disposal:** If possible, shred paper documents that contain personal information rather than just throw them away. Identity thieves have been known to retrieve information from the garbage. Credit card companies, for instance, often include a blank check on bills, which if disposed improperly can be retrieved, Calligan said.

• **Red flag:** Take mail to the post office or a public drop-off rather than leave it in mailboxes at home with the flag up. Identity thieves often see that as an opportunity to steal checks or other documents.

• **Home security:** Be careful with security monitoring companies and other businesses to whom you provide personal data such as bank account numbers, Calligan said. Mergers in various industries put your information in new hands.

• **Social Security:** Don't give out your number unless necessary.