Anatomy of an ID theft

After Heather Harding's identity was stolen, she worked full time to reclaim her good name.

November 18, 2004: 3:24 PM EST
By Joan Caplin, MONEY Magazine

NEW YORK (MONEY Magazine) - The first warning sign came last December, although at the time Heather Harding didn't recognize it as such. Instead, when the letter arrived from Capital One asking if she'd requested a credit application, Harding assumed a simple mistake had been made.

Five months rolled by without incident, but then the red flags popped up in rapid succession. A call from her bank, Wells Fargo, inquiring about her application for a line of credit. The same question from Chase, where she had no accounts. Then a message from a local Ford dealer, who said he hoped to see her later that day with the additional paperwork they had discussed.

Harding knew nothing about these transactions. Instead, she realized, she had become a victim of one of the fastest-growing crimes in the U.S.: identity theft.

The credit inquiries, it turned out, were just the beginning. As Harding would find out over the following months, the thief had also rented a luxury apartment with a pool, a fitness center and views of the Pacific Ocean. She signed up for utilities, cell phones, Internet service and cable. She opened multiple financial accounts and ran up nearly $10,000 in bills.

Yet, though the police are virtually certain they know the thief's true identity, she has not been arrested and probably never will be.

This nightmare, unfortunately, is all too common. Harding, 34, is one of 7 million people who were victims of identity theft in 2003, an increase of 80 percent from the previous 12 months.

At the Federal Trade Commission, identity theft is now the No. 1 consumer complaint. Only a tiny fraction of the perpetrators are prosecuted -- often, as in the case of Harding's alleged thief, because there are no witnesses who actually see the suspect filling out the credit application.

No one knows for sure how the criminal gained access to Harding's Social Security number, which opened the door to the thievery that followed.

What is more important, though, is the decisive action that Harding took afterward on her own

behalf -- steps that ultimately restored her good name and absolved her of any financial responsibility.

Stage 1: Damage control.

Harding took the first crucial steps in wresting back her identity even before she understood properly that she'd been the victim of a crime. At the suggestion of a representative from Capital One, the first lender to contact her last December, Harding notified the police and the three major credit reporting agencies (CRAs) that a false credit application had been made in her name.

She also asked the agencies to place a fraud alert on her credit reports. That would supposedly prompt lenders to inform her of any new requests for credit in her name. In practice, however, it often doesn't work.

In this case, though, Harding received a flurry of unsolicited calls from lenders in May, enough to make her realize that someone was using her identity.

She kicked her damage-control campaign into high gear. She visited the Ford dealer who had left the mysterious phone message about the need for additional paperwork. There, sales manager Othman Ghneim explained that the fraud alert on Harding's credit report had popped up when he ran a check on the young woman who had claimed to be Harding.

His suspicions grew when he perused the report. He says, "I saw some credit there that I didn't think this girl could have. It went back too far -- she would have been about 10 years old."

As she listened to Ghneim describe his encounter with her Doppelganger, Harding got chills.

"She knew everything about me," Harding says. "She knew I was married, where I lived, that I drove a Mercedes. And she had a story for everything."

When Ghneim found no record of Harding having owned the Ford Taurus that the imposter wanted to trade in, for instance, she explained that her husband got the Mercedes in their divorce. The real Harding has been happily married for six years.

But it wasn't until later in the day, when police paid a visit to the impersonator and found out that she lived only 20 minutes away, that Harding (whose home is in a gated community in Orange County, Calif.) got truly scared.

Until that moment, Harding says, she'd been in denial. Now she realized her security was threatened. "She could do something to my house, to my family."

Stage 2: Reality sets in.

Harding quickly put a number of safety measures in place.

She placed passwords on her legitimate financial accounts. She filed a complaint with the FTC, which provides law enforcement officials with information that will help stop perpetrators.

Harding also recontacted the police, and called the CRAs to reactivate her fraud alerts, which

can expire in as little as 90 days. (For more ways to protect yourself, click here).

Filing a fraud alert with one CRA is supposed to automatically trigger all three agencies to send copies of your credit report so you can detect and fix errors.

Harding took no chances and made three separate requests for copies. She received them within a week. The one from Experian, however, was blank. It took several weeks and considerable hounding before the corrected report resurfaced.

Stage 3: Grunt work.

Victims of identity theft can spend anywhere from 30 to 600 hours recovering from the crime. Harding's experience was at the upper end of the spectrum. As is typical, most of Harding's time was spent on phone-hold or in repeated attempts to correct or make headway in matters she thought she'd already corrected or explained.

Overwhelmed by the task at hand, Harding began taking time off from her part-time job as the director of marketing for a special-events firm. A month into her ordeal, she decided to quit for good. Reclaiming her good name had turned into a full-time career.

To stay on top of the job, Harding began keeping a log of action she took to set her credit record straight.

"I've worked in the special-events industry for about 15 years," she explains, "and I know details are extremely important."

Harding's records cover 10 single-spaced pages and a spreadsheet with headings such as "date," "company contact," "time spent" and "response."

Harding sent all her correspondence by certified mail, return receipt requested. Credit agencies, she learned, are required by law to respond within 30 days. If she had her letters time-stamped, in effect, she'd improve her chance of a quick response.

"You need to try to control the situation as much as possible," explains Harding.

Under the circumstances, Harding's quest for control was certainly understandable. In a 2003 study by the Identity Theft Resource Center, 76 percent of the respondents said they experienced "a sense of powerlessness or helplessness." Even more universal was the feeling of rage: 89 percent said they had it, as did Harding.

She began to have trouble sleeping and felt constant anxiety, "One minute, I'd be extremely angry and the next I'd be crying." In time, she even stopped socializing. "People try to understand," she says, "but it's very difficult unless you've been through it."

Creditors began hounding her, demanding payment for goods and services she'd never ordered. Getting out of town with her husband Wes became one of her few pleasures because Harding knew that then she couldn't get any phone calls.

"I was afraid to go to the mailbox or answer the phone," she explains. "I didn't know who'd be threatening me next."

Stage 4: Righting the wrongs.

Over the next four months, Harding vigilantly contacted every company that wrongly appeared on her credit report. She'd call, e-mail or send certified letters -- repeatedly -- until the false information was dropped.

She always identified herself as a victim of identity theft, then supplied the company with a notarized ID Theft Affidavit of the crime (available at ftc.gov).

"I asked as many questions as I could, to try and piece together what [the thief] had done," she says. "I was a real reporter."

The most stressful moment: visiting the apartment complex where the suspect lived, after the manager insisted on a face-to-face meeting.

"I was terrified I'd bump into her," Harding recalls. "I was afraid [the manager] would call her down and confront her." Her worries, though, were unfounded. The imposter never appeared.

Stage 5: Recovery.

One year after Harding first became a victim of identity theft, she has finally managed to clear her name. The fraudulent accounts are closed, the black marks have been erased from her credit record, and some equilibrium has returned to her life.

Charles Juntikka, a New York attorney who specializes in credit report litigation, is impressed with what Harding has accomplished in a short time, but warns that negative data sometimes creep back into the credit reports.

Stay vigilant, Juntikka cautions, and "don't assume that once the problem is fixed, it's fixed for good."

Harding may be in a better position to prevent a recurrence than many other victims because of where she lives. California is one of just two states (Texas is the other) that allow identity-theft victims to put a freeze on their credit reports.

Now the only way a bank or other creditor can run a check on Harding is if she gives her permission via a PIN. Under state law, Harding is also entitled to review her credit reports for free every month for a full year to make sure there is no improper activity.

In the coming year, all consumers will be the beneficiaries of greater protections against identity theft. A nationwide system of fraud detection and alerts that is supposed to take effect Dec. 1 creates procedural standards that CRAs must follow to ensure that future requests for credit are legitimate.

It also allows victims to report the crime with a single call. In addition, between now and September 2005, everyone will be able to begin checking their credit report once a year for free.

Harding will certainly be checking hers. She never wants to feel as out of control as she has this past year; she compares the emotional impact of identity theft to battered person

syndrome.

While she hopes her nightmare has ended, she concedes, "Once you've been through an experience like this, I don't think you ever really know if it's over for good." ■

Find this article at:
http://money.cnn.com/2004/11/18/pf/security_IDrecovery_0412/index.htm

☐ Check the box to include the list of links referenced in the article.