

Identity Theft Hits Home

It Can Happen To You - How To Protect Your Most Valuable Asset

BY DEBRA HAND

When Maria* answered the telephone one afternoon in November 2002, she did not expect to begin a yearlong odyssey to clear her husband's credit rating. The caller was a diligent credit card company employee who had noticed that an application bearing Maria's husband's name listed a Florida address, while a search of his driver's license number, provided as identification, revealed that he was a New York resident.

It turned out that Maria's husband, Michael, a prominent Chappaqua physician, had his identity stolen. Maria immediately contacted the three major credit reporting agencies (Equifax, Experian and Trans Union), which revealed that the thief had already taken out ten to fifteen credit cards in Michael's name since October 2002, after apparently having obtained his name, Social Security number, birth date and driver's license number.

Michael was relatively lucky; by discovering the identity theft quickly and receiving the three credit reports, he was able to have the fraudulently issued credit cards frozen. By placing a fraud alert on his name, each credit-reporting agency would be able to inform credit card companies running application credit checks and contact him for verification of each application.

Michael is just one of many facing this increasingly common problem. Identity theft is the number one consumer fraud in the nation, according to Chappaqua Postmaster General Carolyn Cristantiello. Westchester residents are far from safe. The Westchester County Department of



the various businesses individuals deal with on a regular basis. "They come in with a total sense of vulnerability."

How It Happens

Victims of identity theft rarely do anything out of the ordinary to increase their chances of being targeted. Indeed, Maria believes that her husband's situation likely resulted from their mortgage refinancing earlier in 2002, with an unethical bank employee selling

Michael's personal information on what she has learned is a black market for identity thieves.

Your everyday transactions reveal everything from your name, address and phone number to your date of birth, Social Security number, bank and credit card numbers and even your income. Identity thieves can then obtain this sensitive information in a variety of ways, including: misusing their own employers' (such as banks) access to records or credit reports; bribing employees with access to such information; computer hacking; rummaging through trash receptacles; mail theft (including bank and credit card statements, pre-approved credit offers, new checks and tax information); stealing wallets containing identification, cards, and information; stealing credit and debit card numbers during processing; or posing as officials with legitimate right to your personal information.

Once in possession of your personal information, identity thieves can drain your bank account, go on spending sprees with your existing credit accounts, open new bank and credit card accounts or obtain serv-

Consumer Protection recently listed identity theft as the tenth most common consumer complaint. And Chappaqua is no exception.

"We're finding that identity theft is becoming much more frequent," said Financial Center Manager Christina O'Neill of Chappaqua's Citibank branch. She noted that an increasing number of account holders, and even non-Citibank customers, are coming into the branch having had their identities stolen.

"People are unsure of who they can trust, even through their normal channels," said O'Neill, referring to

"They come in with a complete sense of vulnerability"

—CHRISTINA O'NEILL,
Financial Center Manager,
Citibank, Chappaqua

ices and loans in your name and change the mailing address on your accounts to delay your awareness of the problem.

It can be some time until you discover that your identity has been stolen. Michael was fortunate that a fraudulent credit application fell into the hands of a conscientious employee only one month after the thief began his activities. On the other hand, John, another Chappaqua resident, only learned that his identity had been stolen when he and his wife started receiving collection notices and phone calls from credit card companies they had never heard of. Almost four years later, they are still dealing with the repercussions.

In addition to unexplained charges or withdrawals on your credit card and bank statements, the Federal Trade Commission cautions that other indications of identity theft exist. (See box, *Red Flags of Identity Theft*).

Action to Take

The Westchester County Department of Consumer Protection, the Federal Trade Commission (FTC) and the U.S. Postal Inspection Service all offer similar guidelines on what to do when you learn that your identity has been stolen. It is vitally important to act *immediately* upon suspicion of identity theft, keep copies of all documentation involved in your investigation and follow up all phone calls in writing, by certified mail with return receipt requested. The guidelines include:

Place fraud alerts on and review credit reports. As Maria learned, promptly contacting the fraud divisions of each of the three major

credit reporting bureaus and placing a fraud alert on your credit reports can prevent the identity thief from opening additional accounts in your name. While the FTC guidelines state that one credit bureau will automatically notify the other two, Maria called each one herself and found that each report contained somewhat different information. If you are a victim of suspected identity theft, you will be provided with copies of credit reports free of charge. Carefully review them for evidence of unexplained debts on legitimate accounts, accounts you did not open, inaccuracies in personal information, and mysterious inquiries into your credit.

Close fraudulently opened or tampered accounts. These include not only banks and credit cards, but phone companies, utilities, and similar service providers. Each company's fraud dispute forms (or, if accepted, the ID Theft Affidavit available from the FTC's website) should be executed and returned promptly. Use new personal identification numbers (PINs) and passwords for replacement accounts. If personal checks have been stolen or misused, your bank should notify its check verification company (usually TeleCheck, Certegy, Inc. or International Check Services) to flag your file to refuse further counterfeit checks, and you should look into state laws protecting your liability.

File a police report. Creditors may require a copy of your local police report for validation. The FTC also suggests filing a report with them to help track down and stop identity thieves.

Many banks and credit card companies now offer various services to help consumers deal with the ramifications of identity theft. In response to increasing complaints of identity theft, Citibank, for example, has established "Citi Identity Theft Solutions," a free service offered to its banking and Citi Card customers that help restore credit history. According to O'Neill, identity theft specialists provide immediate support by helping victims stop fraudulent activity, notifying credit bureaus to place fraud alerts, contacting other creditors, closing affected accounts and establishing new accounts with new passwords.



Westchester Senior Postal Inspector Jake Burke and Chappaqua Postmaster Carolyn Cristantiello recently spoke at a Chappaqua Rotary Club luncheon on the Postal Service's role in preventing identity theft.

How to Protect Yourself

As Michael learned, prudence with respect to your personal information is no guarantee that you are immune from identity theft. However, the authorities recommend several steps that you can take to minimize your risk of exposure and damage:

- Never divulge personal information over the telephone or Internet to someone you're unsure of or unless you have initiated the contact. Confirm how your information will be used and secured.
- Protect your accounts (bank, credit and phone) with passwords, avoiding easily available information like your birth date, Social Security or phone number, or mother's maiden name.
- Review credit card and financial statements for unauthorized transactions, immediately reporting anything unusual.
- Secure all personal information in your home, particularly if you have roommates or employ outside help or services.
- Never record credit card, driver's license, Social Security or other account numbers on your personal checks. If necessary, only include the last several numbers of the account.

Phone numbers for the major credit bureaus:

Equifax:

To order report: (800) 685-1111
To report fraud: (800) 525-6285

Experian:

To order report or report fraud:
888-EXPERIAN (39737426)

TransUnion:

To order report: (800) 888-4213
To report fraud: (800) 680-7289

- Promptly remove mail from your mailbox, and avoid leaving outgoing mail in unsecured mail receptacles.
- Confirm security procedures for personal information in your workplace.
- Shred or tear charge receipts, copies of credit applications or offers, insurance forms, physician statements, ATM receipts, checks and bank statements and expired charge cards prior to disposal in the trash.
- Keep your Social Security card in a secure place, never in your wallet.
- Copy the fronts and backs of all credit and bank cards carried in your wallet, and keep in a secure place in your home. Having the customer service telephone numbers readily accessible can be vital if you have to quickly cancel your cards.
- Only carry credit and identification cards that you actually need.
- Keep your wallet in a safe place in your place of employment.

Vicki Birdoff



Never keep your Social Security card in your wallet and secure your purse.

top, and avoid automatic log-in features that save your user name and password.

- Delete personal information stored on your hard drive before you dispose of it.
- Annually order and review copies of your credit reports (particularly if you have been a victim of identity theft in the past) from the three major credit rating bureaus.

Remain Vigilant

Despite the time and aggravation required in calling each company which had issued a card to the identity thief, filling out affidavits and going through elaborate bank identification procedures every time they made a withdrawal or wrote a check, Michael and his family did not really suffer financially as a result of the theft. Some of the companies' investigations took a great deal of time, however, and Maria found that it was her responsibility to follow up by telephone to confirm that the inquiries were proceeding and completed.

During that time, the credit agencies that had placed fraud alerts telephoned to confirm each time a new credit account was opened in Michael's name. It took the better part of a year for the fraud investigations to be completed and Michael's good name restored. While the thief's activities did not

interfere with their application for a home equity loan in connection with home renovation, he apparently used Michael's name and Social Security number to apply for Michael's federal tax refund, which Michael received approximately eight months later.

On the other end of the spectrum, when John applied for a new mortgage in connection with a prospective house purchase almost four years after his identity was stolen, his bank suspected prior identity theft when it appeared that his credit approval rating had mysteriously gone down. John has since installed a firewall on his computer, which is frequently used to make Internet purchases, and can now see daily the number of failed attempts by hackers to access his information.

While no one is guaranteed immunity from identity theft, it is clear that preventive measures and caution can minimize your chances of having your identity stolen. Simple steps now can protect your most valuable asset—your good name.

*Names have been changed to protect identity.

Visit www.ftc.gov and www.westchestergov.com/consumer for further information, important telephone numbers and complete guidelines.

DEBRA HAND is a freelance writer and non-practicing attorney living in Chappaqua who will be checking her statements much more carefully from now on.

It is vitally important to act immediately on suspicion of identity theft.

Secure your Computer

If you frequent the Internet, your computer is likely a source of personal information that must be protected from identity theft as well. The FTC suggests:

- Update virus protection software regularly.
- Never open or download files from strangers.
- Install a firewall, particularly if you have a high-speed "always on" connection to the Internet.
- Use a secure browser, and look for a "lock" icon and privacy policies on any website to which you are submitting personal information.
- Refrain from storing financial or personal information on your lap-

RED FLAGS of Identity Theft

1. Failing to receive bills.
2. Receiving credit cards for which you did not apply.
3. Denial of credit for no reason that you are aware of.
4. Receiving collection notices or calls about services or merchandise you didn't purchase.
5. The FTC also recommends being suspicious of any mail that indicates that an identity thief may have changed your mailing address on your accounts.