SRMG HOT TOPIC: IDENTITY THEFT

Imagine that you are trying to buy your dream home. Your credit history is impeccable, but your bank rejects your loan application because of your poor credit score. You begin to receive bills in the mail for credit cards you never applied for and bounced checks you never wrote. You have fallen victim to the fastest-growing crime in the United States according to the U.S. Department of Justice (DOJ)—identity theft.

Most people don't realize how widespread identity theft has become.

- It is the number one concern for consumers contacting the Federal Trade Commission (FTC), accounting for 21 percent (278,078) of complaints received in 2009 (http://www.ftc.gov/opa/2010/02/2009fraud.shtm).
- About 7.5 percent of adults in the United States lost money as a result of financial fraud in 2008, according to a study by Gartner, Inc. (http://news.cnet.com/8301-1009_3-10186176-83.html). Most of these losses were due to data breaches.
- According to the FTC's *2009 Consumer Sentinel Network Data Book* (http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf), the top five states in terms of victims per capita are Florida, Arizona, Texas, California, and Nevada.

WHAT IS IDENTITY THEFT?

Identity theft involves acquiring key pieces of an individual's personal information—such as his or her name; Social Security number (SSN); address; and date of birth—in order to impersonate him or her. This information enables an identity thief to commit numerous forms of fraud, including opening new bank accounts; taking over the victim's financial accounts; purchasing automobiles; applying for loans, credit cards, and Social Security benefits; renting apartments; and establishing services with utility and telephone companies. A thief can obtain all of this information online, over the telephone, or in person.

Identity theft was declared a federal crime in 1998 with the Identity Theft and Assumption Deterrence Act (http://www.ftc.gov/os/statutes/itada/itadact.htm). Identity theft fraud cases are investigated by federal agencies such as the Federal Bureau of Investigation (FBI; http://www.fbi.gov/); the U.S. Secret Service (http://www.secretservice.gov/); and the U.S. Postal Inspection Service (USPIS; http://postalinspectors.uspis.gov/).

HOW CAN A THIEF OBTAIN YOUR PERSONAL INFORMATION?

Anything that provides access to your personal information is a potential target.

- Your mailbox (bank statements, tax documents, bills, etc.)
- Personal records kept on file with hospitals, landlords, and lenders
- Your computer
- Your telephone
- Public records
- Your garbage

Thieves can also steal your personal information by calling you and pretending to be a bank or credit card company employee or through automated teller machine (ATM) skimmers that record your personal account number and personal identification number (PIN). Be aware, and know how to protect yourself.

HOW TO PROTECT YOURSELF

Education is the best weapon against identity theft. It is imperative that you take steps to learn more about identity theft and how to prevent it from happening to you, your business, or your family. Here are some suggestions to help you minimize your risk and make it more difficult for identity thieves to access your information.

- Review your credit report for changes at least once every year. It contains your SSN, past and present employers, and a listing of your current and past financial accounts.
- Review your monthly credit card statements. Look for changes or charges that you did not make. It's also a good idea to monitor your financial accounts online so that you can view them on a daily basis.
- If you don't receive bills or statements on time or you receive credit cards that you didn't apply for, always call to confirm that there is not a problem.
- Shred any documents that contain personal information, including preapproved credit applications, credit card receipts, and bills.
- Don't give out your SSN. It is the primary target for these types of criminals. Never carry a Social Security card in your purse or wallet.
- Don't leave delivered mail in your mailbox overnight, and drop all outgoing mail off at the post office—especially bills or documents containing personal information.
- Be careful where you store deposit slips and checks, as thieves can use them to access your bank account or write checks to themselves. Always report a lost or stolen checkbook, ATM card, or credit card immediately.
- Don't give out personal information over the telephone unless you initiated the call.
- Empty your wallet of extra credit cards and identification.
- Memorize your SSN and passwords. Never make them easily accessible to others.
- Use caution when disclosing personal information—such as your checking account or credit card numbers—on any Web site unless you receive a secured authentication key from the provider.
- When you subscribe to an online service, it may ask you to provide your personal credit card or bank account information. Be aware when asked to confirm your enrollment by disclosing passwords to your personal accounts.

WHAT TO DO IF IT HAPPENS TO YOU

- Call each of the three credit bureaus' fraud units to report identity theft. Ask the bureaus to put a fraud alert/victim impact statement in your credit file asking that creditors contact you before opening any new accounts. Clone any accounts in your name that were opened without your authority.
- Contact your local police department to report the crime, and ask for a copy of the police report.
- Contact the local USPIS and/or local post office.
- Contact the FTC to report the problem.
- Call your state Department of Motor Vehicles (DMV) to see if they issued another license in your name. If needed, file a DMV complaint form to begin the fraud investigation.

- Contact your bank and credit card companies immediately. If needed, obtain new cards with new passwords or PIN numbers.
- Keep a log of all persons that you contact (with telephone numbers), and photocopy all pertinent documents pertaining to your investigation.

You can report identity theft to several organizations.

TransUnion LLC
http://www.transunion.com/sites/corporate/personal/fraudIdentityTheft.page
1-800-680-7289

Equifax Inc.
http://www.equifax.com/answers/set-fraud-alerts/en_cp
1-800-525-6285

Experian
https://www.experian.com/consumer/cac/InvalidateSession.do?code=SECURITYALERT
1-888-397-3742

FTC
https://www.ftccomplaintassistant.gov/
1-877-ID-THEFT (1-877-438-4338)

Social Security Administration (SSA)
http://www.ssa.gov/oig/hotline/index.htm
1-800-269-0271

USPIS
https://postalinspectors.uspis.gov/forms/idtheft.aspx
1-877-876-2455

Your Local Police Department

MEASURES TO PREVENT IDENTITY THEFT IN THE FUTURE

In the future scientists will develop more secure methods of authentication. These methods—based on biometric technology—will provide a biological authentication of a person, including characteristics of structure and movement such as fingerprints, iris recognition, voice responses, and digital signatures. For example, the characteristics of a person's handwritten signature include not only the actual signature style, but also the pen pressure and the duration of the signing process. Computers will record this information as a digital algorithm, which they will compare against future signatures. For more information, see http://en.wikipedia.org/wiki/Biometrics.