IDENTITY THEFT

Growing and deadly

— BY JOAN TUPPONCE —

Lighthearted ads touting bank services that protect against identity theft may elicit laughs but being robbed of your good name is no joke. Identity theft is a personal invasion clothed in secrecy.

"Identity thieves steal consumers' time, money and security, just as sure as they steal their identifying information, and they cost businesses enormous sums," says Federal Trade Commission Chairman Deborah Platt Majoras.

Identity theft occurs when a person uses another person's identifying information without authorization and with the intent to defraud for his or her own use or the use of a third party.

"This type of crime has really increased in the last five years," says Samuel E. (Gene) Fishel, Senior Assistant Attorney General and chief of the computer crime section of the Virginia Attorney General's Office. "Most of this criminal activity now occurs over the Internet because more people are using the Internet to conduct transactions. Increased Internet commerce has exposed people to a greater risk of identity theft."

Thieves may hack into a company database to steal customer data or send out phishing emails pretending to be a financial institution. "They will often ask you to click on a link and provide your personal information to a website [that they have created] or they might install spyware on your computer," Fishel says. "This is the fastest growing crime in the U.S. because it's easy for criminals to commit."

To guard against this crime, Fishel suggests using anti-virus software and installing a firewall. "You need to make sure you are not clicking on emails from someone you don't know," he says. "Most financial institutions do not conduct business that way. If you get a phishing email, don't click on the links in the email. Immediately delete the email and call your bank."

The Metro Richmond Identity Theft Task Force targets identity theft in all forms, from credit cards to altered or counterfeit checks. An altered check is a good check stolen and changed by the suspect. Counterfeit checks are typically stolen from a victim, copied and cashed or converted by criminals.

PREVENTING IDENTITY THEFT

Five keys from the Metro Richmond Identity Theft Task Force (http://www.richmondidtheft.com):

1. Review your credit report annually. Every individual is entitled to one free credit report each year. Go to www.annualcreditreport.com for more information.
2. Promptly remove mail from your mailbox. Don't leave it in the box overnight.
3. Pay attention to your financial account statement. Know your billing cycles. Review your statements every month.
4. Shred all financial documents when you are finished with them.
5. Never give out personal information to anyone unless you initiate contact. Know who you are dealing with.

THE FEDERAL TRADE COMMISSION ALSO ADVISES:

1. Protect your Social Security number (SSN). Don't carry your Social Security card in your wallet or write your SSN on a check. Give it out only if absolutely necessary or ask to use another identifier.
2. Never click on links sent in unsolicited emails; instead, type in a web address you know. Use fire walls, anti-spyware and anti-virus software to protect your home computer. Visit OnGuardOn line.gov for more information.
3. Don't use an obvious password like your birth date, mother's maiden name or the last four digits of your SSN.
4. Keep your personal information in a secure place at home.

Postal Inspector M. J. Romano of the U.S. Postal Inspection Service

"Forty-five percent of people aged 40 and above are victims of identity theft."

"In Richmond, we're seeing a lot of check fraud," observes Postal Inspector M. J. Romano of the U.S. Postal Inspection Service, the lead agency in the Task Force. "We are also seeing credit card theft and fraud."

Some criminals use old-fashioned methods like stealing bills or incoming mail. "Everybody gets solicitations for new credit cards," Fishel says. "People need to shred credit card solicitations they receive. Be wary of placing bills and checks in your mailbox where any person can come by and steal them."

Romano notes that the percentage of mail theft, "as opposed to theft of credit cards out of wallets and cyber attacks," is low, adding that "the U.S. Mail has always been a safe, secure way of conducting commerce." He advises not leaving mail in your box overnight, placing delivery on hold when on vacation and mailing sensitive items in a blue collection box.

Currently, credit card fraud tops the list of identity theft crime. Each day, millions of Americans hand their cards to store or restaurant staff. What happens when that card is out of your sight could ruin your credit.

"We've also worked cases where people use a high-tech skimming device to read the card after it's been swiped," Romano says. "A thief can retrieve that information and use it to make purchases, or [he or she] can counterfeit the card."

These devices can be installed anywhere you swipe your credit card. Romano suggests looking before swiping. "Look for anything out of the ordinary, a raised device on the card

receiver or anything that looks like it has been modified."

Forty-five percent of people aged 40 and above are victims of identity theft. "Traditionally, those folks were not on the Internet as much as they are now," Romano says, explaining the lower number of victims. "And they may not have been reporting the crime. Now we are seeing more reporting in that age bracket."

Phone and utility fraud (when someone uses your identity to arrange phone and utility services) ties in numbers with bank fraud, which can be committed by someone working for a financial business. Take the 2006 case of Kathryn Feuer, a 41-year-old Richmond woman prosecuted by the Attorney General's Office for fraud and aggravated identity theft.

Feuer was employed by two area businesses to perform accounting services. In her guilty plea, she admitted to devising a scheme to defraud her employers by stealing checks and forging signatures. As part of her sentence, she received a mandatory, consecutive two-year prison term for aggravated identity theft.

Those who commit identity theft get a two-year mandatory sentence in a federal penitentiary for every count on which they are charged, thanks to the federal version of the Aggravated Identity Theft Statute, which falls under the 2004 Identity Theft Penalty Enhancement Act. Romano credits the lower numbers of identity theft in the Richmond area to that statute. "Prior to that, penalties for identity theft were not very strong," he says.

Despite progress, the problem is not going away. According to Richard Swed, an identity theft security specialist with Swed & Associates, financial theft is just one of five areas of identity theft. "The reality is," he says, "that 28 percent of identity theft is financial and 72 percent has nothing to do with your credit report."

Three other areas of identity theft are criminal theft, where a thief uses a stolen Social Security number (SSN) to commit a crime; driver's license theft, where a stolen license is either sold or used as identification; and Social Security theft, where someone without a SSN steals one and uses it to get a job.

The fifth area, medical identity theft, has two facets. When someone uses stolen information to access your medical insurance, "whatever they get treated for is now in your medical file," Swed explains. "If, for example, they get treated for a drug overdose, it's now in your file."

The most disturbing aspect of medical identity theft, according to Swed, occurs when you are admitted to an emergency room and can't communicate to hospital personnel. "They have to rely on your medical files and you could die because of mistreatment based on your files," Swed says.

Everyone is vulnerable to identity theft. "Criminals are always going to be out there, finding new ways to perpetrate identity theft," says Fishel. "The scariest thing is that you cannot control all the information out there on you. That's why it's really important that you be vigilant and monitor your accounts."

Joan Tupponce is a national award-winning writer who writes for local, regional and national publications.

WHEN YOU SUSPECT ID THEFT - FTC TIPS

The Federal Trade Commission offers the following advice for defending yourself against ID theft as soon as you suspect it:

- **Place a "Fraud Alert" on your credit reports and review the reports carefully.**
- **Close accounts. Close any accounts that have been tampered with or established fraudulently.**
- **File a police report with law enforcement officials.**
- **Report the theft to the Federal Trade Commission. Online: ftc.gov/idtheft or by phone at 1-866-438-4338.**