KANAWHA CAPITAL MANAGEMENT, LLC

Fourth Quarter 2013

# KANAWHA CURRENTS

## This Quarter's Highlights



## IDENTITY THEFT: MINIMIZING YOUR RISK

### What is Identity Theft?

Identity theft occurs when someone uses another person's information to commit fraud or other crimes. Information such as your name, Social Security number, credit card number, financial account number, or digital passwords may be used. As many as 9 million Americans have their identity stolen each year.

**How do identity thieves get information?**

- **"Dumpster Diving":** A thief will rummage through trash looking for bills, bank account statements or other papers with personal information on it.
- **"Shoulder Surfing":** A thief will watch from a nearby location as you punch in your credit card number or listen in on your conversation as you give your credit card number over the telephone.
- **Skimming:** A thief will steal credit or debit card numbers in otherwise legitimate transactions by copying receipts or by using a special storage device when processing your card. Common scenarios for skimming are restaurants and retail locations where the skimmer has temporary possession of the victim's credit card.
- **Phishing:** A thief will pretend to be a financial institution or other company and send spam, pop-ups, or phone calls to trick an individual into revealing personal information.
- **Changing Your Address:** A thief will divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing:** A thief walks away with your wallet, purse, or phone. Stealing incoming and outgoing bills from mailboxes is also a common practice of identity thieves.
- **E-mail Hacking:** According to Charles Schwab, over 90% of wire fraud attempts involve scammers using an e-mail account to commit fraud.

**What do identity thieves do with your information?**

The Federal Trade Commission (FTC) lists several ways thieves may use your personal information.

Credit Card Fraud: The thief may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report. A thief may also change the billing address on your credit card so that you no longer receive bills and then may run up charges on the account.

Because your bills are sent to a different address, it may be some time before you realize that there is a problem.

Phone or Utilities Fraud: The thief may open a new cellular account in your name or run up charges on an existing account. The thief may also use your name in order to get utility services such as electricity, heating, or cable television.

Bank/Finance Fraud: A thief may create counterfeit checks using your bank checking account or open new loans in your name to gain access to funds. A thief may also clone your ATM or debit card and make electronic withdrawals, draining your account. A thief may give fraudulent wire instructions in your name. The fraudsters sometimes even have the ability to produce a letter of authorization for the wire request.

Government Documents Fraud: A thief may get a driver's license or official ID card issued in your name, but with the thief's picture. A thief may also use your name and Social Security number to get government benefits or file a fraudulent tax return to get your tax refund.

## Detecting Identity Theft

Unfortunately, many consumers find out that they are a victim of identity theft after damage has already been done.

**What are common signs of identity theft?**

- Accounts you didn't open and debts on your accounts that you did not incur
- Unexplained withdrawals from your bank account
- Inaccurate information on your credit report, such as an incorrect Social Security number, address, name or initials, or employer
- Failing to receive bills or other mail that you normally receive
- Receiving credit cards that you did not apply for
- Being denied credit or being offered less favorable credit terms, such as a high interest rate
- Receiving calls or letters from debt collectors about merchandise or services you did not buy

## Recovering from Identity Theft

If you are a victim of identity theft, consider taking the following steps as soon as possible. It is important that you keep a record with the details of your correspondence, such as whom you spoke to and what the agreed upon resolution was. Start with contacting the companies with whom you have financial relationships (bank, credit card, brokerage/investment advisor, insurance, etc.) and informing them that your accounts have been compromised.

- *Close the accounts that you know or believe have been tampered with or opened fraudulently.* For unauthorized accounts, you can either file a dispute directly with the company or file a report with the police.
- *Review your credit reports.* You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months.
- *Place a fraud alert on your credit reports.* Fraud alerts can help prevent more damage from occurring, by preventing an identity thief from opening more accounts in your name. There are two types of fraud alerts, an initial alert and an extended alert. An initial alert stays on your credit report for at least 90 days while an extended alert stays on your credit report for seven years. To place a fraud alert on your credit file, you only need to contact one of the three consumer reporting agencies; TransUnion, Equifax, or Experian.
- *Create an Identity Theft Report by contacting the Federal Trade Commission and your local police department.* This may give you additional protection by allowing you to remove fraudulent information from your credit report and preventing a company from collecting debts that result from identity theft.

## Preventing Identity Theft

While no precautionary measure can guarantee full protection from identity theft, you can minimize your risk and the potential damage by making it more difficult for identity thieves to access your personal information. The Federal Trade Commission has identified proactive steps individuals should take to reduce their risk.

**Consider a credit report security freeze.**

- ✓ Security freezes can help protect consumers from identity theft *before* it happens. Many states allow you to place a security freeze on your credit report from the individual credit reporting agencies.

- ✓ A credit report security freeze generally allows a consumer to block access to his or her credit report by third parties (such as credit lenders or other companies) who are not exempted under law. Companies with which you have an existing account such as your mortgage holder or credit card company as well as law enforcement and trial courts may be exempted.

- ✓ Be aware that security freezes may involve some tradeoffs. Freezes may delay, interfere with, or prohibit the timely approval of new loans, credit, employment, investments, cellular phone service, utility service, internet credit card transactions, and extension of in-store credit. In addition, a freeze will not prevent a thief from fraudulently using your existing credit card or bank accounts. Therefore, you should continue to regularly check your monthly bank account and credit card statements for signs of any suspicious activity.

**Protect your Social Security number.**

- ✓ Don't carry your Social Security card in your wallet or purse. Don't write your Social Security number on a check.

- ✓ Give your Social Security number only when absolutely necessary and ask to use other types of identifiers when your Social Security number is requested.

- ✓ Your employer and financial institutions will need your Social Security number for wage, tax reporting, and to comply with the Patriot Act. However, sometimes businesses simply want your Social Security number for general record keeping. If someone asks you for your Social Security number, ask them why they need it, how they will use it, and how they plan to protect it from being stolen.

**Treat your trash and mail carefully.**

- ✓ Always shred your charge receipts, copies of credit applications, insurance forms, physicians' statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. Shredding these documents will spoil the endeavors of identity thieves who are picking through trash or recycle bins to find personal information.

- ✓ Mail that is received by you should be promptly removed from your mailbox. If you are planning to go on vacation, contact the United States Postal Service to request that your mail is held while you are unable to pick up your mail.

- ✓ You can reduce the amount of mail that you receive that requires shredding by opting out of prescreened offers of credit. To opt out of receiving these offers, call 1-888-5-OPT-OUT (1-888-567-8688). When you call you will be asked for your Social Security number. This is needed by the consumer reporting agencies to match you with your file.

- ✓ You should be conscious of how you are handling outgoing mail. If you are sending mail that contains personal information, drop it off at your local post office or in a post office collection box rather than leaving it in your unsecured mailbox.

**Be on guard when using the internet.**

- ✓ While the internet provides the benefit of ready access to information and countless services, it also may leave you vulnerable to online scammers and identity thieves. Always use anti-virus and anti-spyware software, a firewall program, and protect any wireless networks from outside users. Configure your computer's operating system and browser to receive updates automatically. The use of older operating systems and software may make you more vulnerable to attack.

- ✓ Be cautious using public computers and use only wireless networks you trust. Your information may be vulnerable when you login to an unsecured wireless network.

- ✓ Don't provide your personal information through a company's web site until you have checked for indicators that the site is secure. One indicator is a lock icon on the browser's status bar. Another indicator is a web site URL that begins with "https." The "s" stands for secure.

- ✓ Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

- ✓ It is also important that you read the privacy policy on a website. The privacy policy should explain how your information will be used and protected.

**Select secure user IDs and intricate passwords.**

- ✓ The personal information you access online should be protected by a user ID and password. You should not use your Social Security number or some variation of this number as a user ID. You should select passwords that are intricate. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers. Combinations of letters, numbers, and special characters make the strongest passwords. Don't use the same password for many of your accounts.

**Verify sources before sharing information.**

- ✓ Don't give out personal information on the phone, through the mail, or on the internet unless you've initiated the contact and are sure you know who you are dealing with. Identity thieves are witty. They may pose as representatives of banks, internet service providers, and even government agencies to get people to reveal their personal information.

- ✓ To confirm that you are dealing with a legitimate organization, check the organization's website by typing its URL in the address line, rather than cutting and pasting it or clicking on a link. Many companies will post alerts if they are aware their name is being used in a scam. You can also call customer service using the number listed in the telephone book to verify whether or not the request for information is legitimate.

**Safeguard your purse, wallet, and smartphone.**

- ✓ Protect your purse, wallet, and smartphone at all times. Carry only the identification information and the credit or debit cards that you'll actually need when you go out. Utilize an automated security lock feature on your smartphone in the event it is lost or stolen.

**Store information in secure locations.**

- ✓ Keep your information in a secure place at your home and office, especially if you employ outside help or are having work done on your home. Share your personal information only with those family members who have a legitimate need for it.

## What We Do to Protect You

Kanawha has in place internal policies and procedures to protect your privacy and prevent identity theft. We do not disclose your personal information to anyone unless it is required by law, is at your discretion, or is necessary to provide you with our services. Our *Identity Theft Prevention Program* is designed to prevent and mitigate identity theft in connection with client accounts. We focus on a series of "red flags" to detect patterns, practices, and activities that indicate the risk of identity theft and the fraudulent use by third parties of our clients' identifying information. We shred all discarded materials containing client information. Copies of both our *Client Privacy Statement* and *Identity Theft Prevention Program* may be obtained upon request. You may find an extended version of this Kanawha Currents piece on our website at http://www.kancap.com/news/currents.

Sources: U.S. Federal Trade Commission, Securian Financial Group, U.S. Department of Justice, Internal Revenue Service, Charles Schwab & Company, Inc., Office of the Attorney General, Commonwealth of Virginia.