KANAWHA
CAPITAL MANAGEMENT
Third Quarter 2019

This Quarter's Highlights

Kanawha Currents

IDENTITY THEFT: MINIMIZING YOUR RISK

What is Identity Theft?

Identity theft occurs when someone uses your personal 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 to fraudulently make unauthorized purchases, open new accounts, or obtain tax refunds.

How do identity thieves get information?

- **"Dumpster Diving":** A thief rummages through trash looking for bills, bank account statements or other papers containing personal information.
- **E-mail Hacking:** An online thief gains unauthorized access to your email. In addition to having your personal and confidential information exposed, they can send electronic requests impersonating you. According to Charles Schwab, over 90% of wire fraud attempts involve scammers using an email account to commit fraud.
- **Mail Theft:** Criminals often target mailboxes, especially those flagged with outgoing mail which may contain paper checks for bill payments.
- **Malware Activity:** Malicious software which penetrates your computer or digital network with the intent to damage and/or steal your data without your knowledge.
- **Mobile Phone Theft:** Smartphones may contain significant amounts of personal data that can be easily accessed if the phone is left unprotected and without automatic security lock features.
- **Old-Fashioned Stealing:** A criminal walks away with your wallet, purse, or phone.
- **Phishing:** A thief pretends to be a financial institution or other company and sends spam, pop-ups, or phone calls to trick an individual into revealing personal information.
- **Skimming:** Stealing credit or debit card numbers in otherwise legitimate transactions by copying receipts or by using a special storage devices when processing your card. This often occurs at retail locations and ATMs where the skimmer has temporary possession of the victim's credit card or cameras are put in place to capture card numbers.
- **Wifi Hacking:** When someone gains unauthorized access to your home or office Wifi network.

What do identity thieves do with your information?

Tax Related Fraud: A criminal uses your personal information to file an income tax return in order to get a tax refund.

Credit Card Fraud: The thief may use your lost or stolen physical card or account numbers and security codes to make unauthorized transactions.

Phone or Utilities Fraud: The thief may open a new cellular account or other utility

service account in your name and accrue charges without your knowledge.

Bank/Finance Fraud: A thief may use your personal information to get control of existing financial accounts or open new loan accounts. They may also create counterfeit checks using your bank checking account to gain access to funds. Additionally, thieves commonly make Federal wire requests that are disguised as legitimate instructions, often via email.

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 obtain government benefits.

Reducing Your Risk of Identity Theft

While no precautionary measure can guarantee full protection from identity theft, there are several ways you can minimize your risk and the potential damage by making it more difficult for identity thieves to access your personal information.

Consider a credit freeze.

- ✓ A credit freeze, also known as a security freeze, can help protect consumers from identity theft before it happens. It is a free tool designed to lock down your credit so that thieves cannot open new credit accounts in your name. Many states allow you to place a security freeze on your credit report from the individual credit reporting agencies.
- ✓ A credit 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. Credit freezes may be lifted by contacting the credit agencies by phone, online, or mail. While freezes may protect you from new accounts being fraudulently opened in your name, they will not prevent criminals from compromising your existing credit card or other financial accounts. Therefore, you should continue to regularly check your monthly bank account and credit card statements for signs of any suspicious activity.

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. It is a good idea to lock your physical documents and records in a safe place at home and back up your digital files in the event your computer or network is compromised.

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. 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, medical statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- ✓ Destroy labels on prescription pill containers prior to throwing them away.
- ✓ 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 1-888-5OPTOUT (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. Consider using encryption software to protect your online transactions.
- ✓ 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 website 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 website 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. Consider taking advantage of two-factor authentication where possible for an additional layer of security protection.

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 whom you are dealing with. Identity thieves 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.

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.

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
- 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
- Being a victim of a security breach with a company you do business with
- Receiving medical bills for services you did not use

Recovering from Identity Theft

If you are a victim of identity theft, it's important to take action immediately. Start with contacting the known companies involved and also reach out to other financial companies with whom you have relationships. Inform them that you have been the victim of identity theft and your accounts have been compromised. Keep a record with the details of your correspondence, such as whom you spoke to and the agreed upon resolution. You should also consider taking these additional steps.

- 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.
- Place a fraud alert on your credit reports. Fraud alerts can help prevent additional damage from occurring by preventing an identity thief from opening more accounts in your name for one year. An extended fraud alert provides this protection for seven years. Fraud alerts require companies to verify your identify prior to issuing credit. 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. Visit www.identitytheft.gov for additional resources.
- Change your electronic login information such as usernames and passwords, as well as PINs for your financial accounts.
- 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.

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.

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, Experian, LifeLock.