
## CUSTOMER AWARENESS

Your confidential information is one of the most valuable things you have. There are many known techniques and social engineering ploys that continually expand the way criminals use to steal your confidential information. With this you may find everyday activities more difficult without educating yourself of ongoing scams. The stress and financial costs from your compromised confidential information can last for years. First National Bank of Mount Vernon has provided this information to help you protect your identity. It includes a number of quick and easy tips you can use to reduce the risk of becoming a victim of identity theft.

## SECURITY CONCERNS

You are responsible to ensure your information security while online, by telephone, or in person. Pay attention and educate yourself about the common techniques used by criminals. Our bank will never contact you about your usernames, passwords, or any online banking information. Once your identity has been stolen it can be almost impossible to recover. Some of the things that criminals may be able to do with your identity include:

- tricking banks or financial institutions into giving them access to your money and other accounts
- opening new accounts and accumulating large debts in your name leaving a negative effect on your credit rating
- taking control of your accounts including by changing the address on your credit card or other accounts so you don't receive statements and don't know of a problem
- opening a phone, internet or other service account in your name
- claiming government benefits in your name
- file fraudulent claims for tax refunds in your name and preventing you from being able to file your legitimate return
- using your name to plan or commit criminal activity
- pretending to be you to embarrass or misrepresent you, including through social media

## TARGETED CONFIDENTIAL INFORMATION

**Personal Information -** information that can reasonably be used to identify a person. Your name and address are obvious examples. In some cases, your date of birth and postal code may be enough to identify you. Personal information can also include:

- social security number
- bank account details
- photographs and/or videos
- social media
- where you work

**Personal Document -** document that contains information about you. Examples include:

- phone, bank, credit card and utility bills
- medical records
- tax refund notices
- home ownership deeds
- rental agreements

**Identity Credential –** any personal document that is commonly requested by governments and businesses as evidence that you are who you say you are. It contains personal information about you, such as your name, date of birth, and address. Examples include:

- social security card
- passport

- birth certificate
- driver license

## THEFT OF CONFIDENTIAL INFORMATION

Your identity can also be stolen if thieves gain access to your personal information. Even if you think thieves only have a small amount of information about you, they can use public sources like social media to find out additional personal information about you, including photographs, your date and place of birth and even information about your family. This can be enough to apply for services, such as a new bank account. They can also use your personal information to create fake identity credentials in your name or even apply for real identity credentials in your name, but with their photograph. Examples include:

- you lose your purse, wallet or handbag or it is stolen
- your home is broken into and personal documents are stolen
- thieves steal mail from your unsecured mailbox
- thieves steal mail, information or personal documents from your trash
- you provide personal information over the phone or internet to what appears to be a legitimate business, but it is actually a scam
- information about you stored on your infected computer system is illegally accessed by criminals
- your online account is compromised
- your personal information is retrieved from social media

## SAFEGUARDING YOUR CONFIDENTIAL INFORMATION

**Carry Only Essential Personal Documents -** Try not to regularly carry important documents, such as your social security card or passport, outside of your home to reduce the risk of them being lost or stolen.

**Destroy Personal Documents -** Destroy documents, such as bills, identity credentials and credit cards before you throw them out. Best practices to destroy documents include shredding or burning.

**Store Personal Identity In Secure Location -** Always store your social security card, birth certificate, and/or passport in a secure location. Make copies of your identity credentials, including your driver license and keep these copies in a secure location as well. The copies could be useful in re-issuing the originals if they go missing or are destroyed. They may also help you to verify your identity. Consider storing all important documents and copies in a fire/water proof secure container or safe deposit box. Make sure documents stored electronically, such as copies of identity credentials, are secure. Strong passwords, encrypted files or trusted data vault websites are all options for secure electronic storage.

**Secure Your Mail -** Remove mail from your mailbox as soon as possible or use a secure post office box. Only send mail at secure, official post office boxes. Notify businesses and friends when you change addresses as soon as possible. Organizations you should inform include:

- government agencies
- banks
- credit and store-card companies
- utility providers
- employer
- accountant
- university or school
- health care providers
- insurance companies
- sports clubs

**Annual Credit Report -** To order, visit annualcreditreport.com, call 1-877-322-8228. Or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three nationwide credit reporting companies individually. They are providing free annual credit reports only through annualcreditreport.com, 1-877-322-8228 or mailing to Annual Credit Report Request Service.

**Check Your Account Information Regularly -** Check all transactions on your banking and credit card accounts regularly. You may be able to detect potential identity theft early and limit the losses.

**Protect Your Computer -** Criminals are continually developing new viruses and programs to steal or access your personal information. To help secure your computer from unauthorized access you need reputable security software. The security software package should include virus, malware/spyware protection and a firewall. Make sure the security software is set to update automatically and that you regularly scan your computer's files. Ensure you renew your security software when the subscription is due. Ensure you only download programs from known, reliable sources. Ensure your operating system, software, browser versions and plug-ins are current.

**Confidential Information On Secure Websites Only -** Avoid entering personal information or a password on an unsecured website. The address of secure websites, such as online banking, will start with "https://" not "http://".

**Use Passwords and Access Controls -** Protect your computer and important documents with passwords and access controls. This is particularly important if you have a wireless network. Ensure you change your passwords regularly and that they contain a mixture of upper and lower case letters, numbers and special characters. Strong passwords which are unique and unpredictable are less likely to be cracked.

**Protect Your Passwords -** Memorize your passwords and personal identification number (PIN) or store them in a safe place. Don't write your passwords down and leave them in an obvious place, such as your wallet, in your desk drawer, or in a file on your computer. Don't share them with friends or family. Never select the option 'would you like the computer to remember this password' when logging onto a website. Periodically change your password.

**Passwords and Usernames -** Use alternative passwords and usernames for different websites, particularly those for sensitive transactions such as banking. Even if one account is compromised the others won't be as vulnerable to hacking.

**Think Before You Click -** Avoid opening attachments or clicking on links in e-mails, unless you are expecting or verify with the email source. Attachments and links can download malicious software into your computer or can redirect you to a fake site. It is best to type in the web address yourself than to follow a link. If you receive an email asking for personal details from what looks like a trusted source, don't hit 'reply' – it could be a scam that is impersonating the trusted source. Answer with a new email message using an email address that you have safely used before or trust. Consider contacting the sender by phone or in person to check if the request is legitimate.

**Social Networking Safety -** Criminals can use information on social networking sites to steal your identity. Make sure you set your social network profile to 'private'. Be cautious about which 'friend' requests you accept. Ideally you should only accept 'friend' requests from people you have met in real life. Think before you post – expect that people other than your friends can see the information you post online. Don't post information that would make you or your family vulnerable – such as photographs, your date of birth, address, information about your daily routine, holiday plans, or your children's schools. If you receive an unusual request from a friend check directly with the friend and do some research to confirm it is legitimate. Beware of scams on social networking sites, such as expensive gifts in exchange for filling out a survey. The survey could be used by scammers to collect your personal information and you may never receive the gift. They could also use it to hijack your account and spam your friends. Be wary of ads posted on the internet, like job ads on social networking sites.

**Avoid Using Public Computers To Access Personal Information -** Personal information, like passwords, can be retrieved from a computer's hard drive. Limit your use of public computers for sensitive transactions, such as accessing email accounts. If you do use a public computer, check to see if the service provider has any security settings. Always remember to clear the history and close the web browser before you leave the terminal.

**Computer Remote Access Request**

If you receive an unexpected call from an internet service providers, telecommunication companies or software providers, do not give them remote access to your computer. Remote

access gives identity thieves unlimited access to steal any personal information you have stored on your computer.

**Safe Computer Disposal**
Make sure no personal information is left on your computer when you sell or dispose of it. Deleted files can sometimes be recovered so you should consider using a data destruction service.

**Lottery Scams**
If an offer sounds too good to be true, it probably is. Be cautious if you've won a lottery you never entered. Ask questions if you have concerns. Don't agree to anything straight away. If you think the offer is legitimate, carry out some independent research before committing yourself.

**Online Dating**
Identity thieves can use dating websites to steal information from you. If someone asks you for bank or personal details, money or gifts you should always exercise caution and consider the possibility that it may be a scam, even if you think you know the person well.

**Mobile Phone Information Security**
Information stored on mobile or wireless devices is at risk of physical or electronic theft. Protect the personal details stored on mobile phones or wireless devices. Use a password or PIN. Turn off wireless features when you aren't using them and only connect to secure (encrypted) wireless networks. Only download applications from official stores or trusted sources. Smartphones are susceptible to malicious software attacks so consider anti-virus software for your phone. Make sure no personal information is left on your phone when you dispose of it. Check with your telephone's manufacturer for instructions on how to delete information.

**Telephone Calls - Personal or Financial Information**
If you receive an unexpected phone call from someone wanting to know your personal details hang up. Banks and financial institutions may contact you if there is suspected fraudulent activity with your account. If you do need to provide personal information over the phone, hang up and contact the organization through the advertised number on their website or in the phone directory only.

**Contact the Do Not Call Register**
The Do Not Call Register allows individuals to register if they do not want to receive unsolicited telemarketing calls. Register via the website https://www.donotcall.gov/ or calling 1-888-382-1222.

## SIGNS OF IDENTITY THEFT

You may not even know you are a victim of identity theft until long after it has happened. You should look for these warning signs:

- calls from creditors, debt collectors about transactions you didn't enter into or debts that are not yours
- arrival of new credit cards that you did not request
- unexpected denial of credit
- refusal of services or benefits because you are informed you are already receiving them
- mail you were expecting, such as bills, not arriving or a reduction in mail
- arrival of bills for goods or services you did not order
- unfamiliar charges or withdrawals on your credit or bank card
- lost wallet, purse or identity credentials – even if you lose them and they are returned they could have been copied

## IDENTITY THEFT REPAIR KIT

You may download a PDF to assist you with Identity Theft on our website https://www.fnbmv.com/security and follow the helpful checklist included.

## SUMMARY

Protecting your identity can seem complicated, so here are 10 simple identity security tips:
1. Secure your personal documents while at home, when you are travelling and if they should be destroyed.
2. Secure your computer and mobile phone with security software and strong passwords and avoid using public computers for sensitive activities.
3. Be cautious about using social media and limit the amount of personal information you publish online.
4. Secure your computer and mobile phone with security software and strong passwords and avoid using public computers for sensitive activities.
5. Learn how to avoid common scams at https://www.consumer.ftc.gov/topics/privacy-identity-online-security
6. Be cautious about requests for your personal information over the internet, telephone and in person in case it is a scam.
7. Investigate the arrival of new credit cards you didn't ask for or bills for goods and services that you did not request.
8. Be alert for any unusual bank transactions or missing mail.
9. If you are a victim of Identity Theft – report it to the police and any relevant organizations.
10. Order a free copy of your credit report from a credit reporting agency on a regular basis, particularly if your identity has been stolen.