Consumer Fraud Frequently Asked Questions

How can I be proactive in protecting my privacy?

- Read all of your statements carefully keeping a close eye on anything that looks suspicious.
- Keep all of your statements in a safe place.
- You can receive a free credit report once a year. Check to make sure all information is accurate and any accounts you have closed are reflected on your report.
- Never provide any account information over the phone or online, unless you have initiated the process.

Is online banking safe despite all the online scams?

- Online banking is an efficient and safe way to handle your money. However, you must be cautious when viewing your accounts. If you are using a public computer such as a library or school PC, make sure you are COMPLETELY logged out of your online banking session when you are finished. Most importantly, confirm that the site you are on is secure. This can be easily identified by the yellow lock in the bottom right hand corner of your browser window. You can also identify a secure site by the "https:" at the beginning of the web address and the yellow lock by the address bar.

What is phishing?

- Phishing involves bogus email messages that use legitimate materials, such as a company's website logo, to entice email recipients to provide personal information such as credit card and social security numbers.

How do I recognize email fraud?

- It is almost impossible to visually identify a phony email. People who create fraudulent sites usually steal corporate logos and graphics to trick their prey. The only way to protect yourself is to never respond to an unsolicited email that asks for detailed personal or financial information.

Can I get a virus or "Trojan Horse" from phished emails?

- Yes. "Smart Hackers" can install programs called "key generators" or “key loggers” that secretly install on your computer without your knowledge. These programs can capture your credit card numbers, user names and passwords, and Social Security Numbers.

How can I avoid "key generators" or “key loggers” from being downloaded on my PC?

- Change your passwords regularly. It is recommended that you change them every 30 days.
- Install anti-virus, anti-spyware, and personal firewall software.
- Update your virus software. Just because you have it installed does not mean it will protect your PC. Contact the manufacturer to determine the most efficient way to keep your virus definitions up-to-date.

How do I protect my credit/debit card?

- Make sure your financial institution has your current phone number so you can be reached if there has been a suspicious pattern of charges on your card.
- Keep a record of your last five transactions in the event you're asked about them.
- If you are notified about suspicious activity on your account, give no information over the phone or internet. Take the representative's name and call back using the number on the back of your credit/debit card.

Who do I contact if there is fraudulent activity on my credit/debit card?

- Call the phone number located on the back of your *credit card* to report any suspicious activity.
- If you believe your *debit card* or PIN has been lost of stolen, or that someone has transferred money or may transfer money from your account without your permission, notify First National Bank’s Customer Service Center **immediately** at 618-939-3792.

How do I know if a check is fraudulent?

- There is no easy way of detecting if a check is fraudulent. If someone over pays you with a check and asks you to deposit the check into your checking/savings account then wire them the difference, it is a great possibility that it is a fraudulent check.

How can I avoid being a victim of check scams?

- Before depositing the check, you can bring it into any of our banking centers and have a teller contact the financial institution that the check was drawn on.

Who is responsible for the loss to my account?

- Bank employees have no way of determining a fraudulent check that looks legitimate. You are responsible for the items you deposit into your account.

Please contact us at 618-939-6194 if you become aware of a scam or believe you are a victim of any of these types of fraud. You may also contact us if you have any questions regarding fraud.