Preventing Fraud

Rapid advances in technology and creative criminal minds make fraud a potentially serious threat on a variety of fronts.

WHAT FIRST FEDERAL BANK IS DOING

Protecting your finances is our top priority. That's why we closely monitor all types of white collar crime, including identity theft and the rapidly growing area of mortgage fraud.

Securing your financial information is essential to protecting your finances. The only employees who see your information are those whose job functions require them to review sensitive data. All employee access is reviewed on a regular basis. Other First Federal Bank's security measures include:

- A commitment by all First Federal Bank employees to our standard of conduct
- Strict procedures
- Annual completion of security awareness training
- Annual completion of privacy policy training
- Fraud monitoring
- Layers of technical protection including:
    - Anti-virus software that shields computers from malicious programs. We also have firewalls and prevention systems that stop unauthorized access to our network and computers, plus secure network protocols that ensure secure connections between our office, partners and customers.

WHAT CONSUMERS CAN DO

Protecting your finances is our top priority. That's why we urge you to join us in preventing fraud. Please review the information below to learn how you can avoid becoming a victim of financial fraud and identity theft:

- Protect Personal Information - Read how to how to avoid email scams and how to protect personal information such as credit card and bank account numbers.
- Use ATMs safely by:
    - Selecting an unusual personal identification number (PIN) to reduce the chance that others can guess your PIN.
    - Keeping your PIN a secret.
    - Do not give out your PIN over the phone.

    - Memorizing your PIN. Do not write it on your ATM card or on anything you carry in your purse or wallet.
    - When using an ATM, use your body as a shield to prevent others from seeing your PIN on the ATM screen.
    - Using ATMs with surveillance cameras.
    - Avoiding any ATM that does not look genuine or appears to have been modified in any way.
- Secure your computer by:
    - Installing an anti-virus program and update it on a regular basis.
    - Updating your software and operating system on a regular basis.
    - Applying all software fixes (also called patches, hot fixes, or service packs) as soon as possible.
    - Using the most current version of your Web browser.
    - Installing a firewall and keep it "on" at all times.

Detecting Fraud

Fraud costs everyone time and money. Detecting fraud is one effective way to avoid becoming a victim or to stop fraud before it goes too far. Click the links below to learn how you can detect possible instances of fraud and identity theft.

- **Check Fraud** - Defines forgery and counterfeiting and shows how to identify these activities.
- **ATM/Debit Fraud** - Explains how to monitor your accounts and recognize unauthorized transactions.
- **Internet Fraud** - Lists specific types of online fraud such as phishing, pop-up ads, keylogging, and spyware. This section provides you with the information you need to avoid Internet scams.
- **Identity Theft** - Defines impersonation and lists steps you can take to prevent this crime.
- **Mortgage Fraud** - Explains this crime and shows you how to monitor credit reports and review documents in order to avoid becoming a victim of mortgage scams.

Check and ATM Fraud

CHECK FRAUD

From counterfeiting to forgery, check fraud affects millions of individuals and businesses every year:

- Counterfeiters create or duplicate checks with your account information.
- Forgers steal your checks, sign or endorse them and then try to cash them.

TO DETECT CHECK FRAUD:

- Use your monthly bank statements to monitor account activity.
- Compare receipts or check carbons against bank statements to make sure the transactions match.
- Ensure that you recognize all charges. If you see suspicious transactions, contact First Federal Bank immediately.
- If you are denied credit, find out why and request a copy of your credit report.
- Check your credit by ordering a free annual report from Annual Credit Report.com.

ATM/DEBIT FRAUD

ATM/debit fraud occurs when criminals acquire your card or PIN number to access your bank accounts and withdraw money.

To detect ATM/debit fraud:

- Use your monthly bank statements to monitor account activity.
- Check sales/ATM receipts against bank statements to make sure the transactions match.
- Ensure that you recognize all charges. If you see suspicious transactions, contact First Federal Bank immediately.

Internet Fraud

EMAIL FRAUD OR PHISHING

Phishing or spoofing occurs when criminals send email messages that appear to represent a legitimate business such as a bank or retailer. Their goal is to trick you into providing confidential information such as account numbers, passwords, card numbers, and PINs. Criminals who obtain this information use it to engage in financial fraud or steal your identity. **First Federal Bank will never ask you to send confidential information via email.**

Fraudulent emails are hard to detect because they use an address, style, wording, logos, and graphics that make them look legitimate. Often, these emails include links to fake websites or launch pop-up windows that are used to collect personal information.

The items listed below are often found in fraudulent emails:

- Urgent messages threatening account closure if you do not act immediately.
- Requests for personal information such as PINs, credit card numbers, social security numbers or any sensitive information. First Federal Bank will never ask you for this information in an email.
- Claims that the bank has lost your confidential information due to a system failure or system upgrade and therefore needs you to provide this information. First Federal will never seek this information via email because we employ an extensive backup system of all essential data.
- Typos, grammatical errors, or incorrect usage of First Federal's name.

PHONE OR FAX PHISHING

Phishing has expanded to phones. Automated phone dialers and voice over IP phone systems are easy to set up and provide criminals with alternatives to email-based phishing.

Voice phishing occurs when you receive a phone call with an automated message instructing you to call another toll-free phone number. The claim is that you must call to address an urgent matter, such as preventing your account from being closed. When you return the call, you are asked to reveal personal information.

If you receive a call like this:

1. Realize that the number displayed on your caller ID can be spoofed and may show First Federal.
2. Do not return the call.
3. Contact First Federal directly for information.

Fax phishing occurs when you receive a fax instructing you to send personal information to a designated number in order to address an urgent matter such as preventing your account from being closed. The tone of a phishing fax is similar to email phishing messages. First Federal Bank will never ask you to send confidential information via fax.

POP-UP ADS

Pop-ups are advertisements that appear in small pop-up windows when you visit a website. These ads are designed to integrate with the Web page or to look like legitimate programs. When you click on some of these pop-ups, you may unknowingly download and install viruses, spyware, or other malicious software. First Federal Bank will never display a pop-up message asking you to verify your personal information.

SPYWARE AND VIRUSES

Spyware and viruses are malicious programs that are installed on your computer without your knowledge. Viruses can damage your operating system while spyware may allow thieves to steal confidential information stored on your computer.

FREEWARE/SHAREWARE/KEYLOGGERS

Keyloggers and Trojans allow criminals to gain access to your computer. Often, they are embedded in free software that you download from the Internet. Only download software from companies and websites that you trust.

SECURE YOUR COMPUTER

Fraud may extend beyond e-mail and the Internet right to your own computer. Take these steps to prevent others from gaining access to your personal computer:

- Install an anti-virus program and update it on a regular basis.
- Update your software and operating system on a regular basis.
- Apply all software fixes (also called patches, hot fixes or service packs) as soon as possible.
- Use the most current version of your Web browser.
- Install a firewall and keep it on at all times.

ID Theft

Identity theft occurs when someone acquires your personal information in order to impersonate you. This information might include your:

- Name
- Date of birth
- Social security number
- Mother's maiden name

Fraud occurs when criminals access your bank accounts or open new accounts, obtain loans in your name and make purchases using your identity.

To detect identity theft:

- Use your monthly bank statements to monitor account activity.
- Check debit, credit card and ATM receipts against bank statements to make sure the transactions match.
- Ensure that you recognize all charges. If you see suspicious transactions, contact First Federal Bank immediately.
- Monitor your credit report regularly.
- Log into online banking to review and confirm recent transactions.

Victims of Fraud

Fraud victims should immediately report theft or any unauthorized activity involving their credit, accounts or identity.

- Contact First Federal's Customer Service
- Please contact the credit bureau if you have been a victim of any scam involving your credit.
- If someone has stolen or forged your checks, fill out the obligatory forgery affidavits with First Federal Bank; there is not cost to you.
- Please call First Federal Bank for information about reporting identity theft, ATM fraud or mortgage scams.