Fraud Prevention Checklist

Fraudulent scams are one of today's fastest growing crimes. Here are some helpful tips to avoid becoming a victim of identity theft:

Stay Alert to Threats & Learn How to Identify Red Flags

- ☑ Scammers may pose as a government official, law enforcement or even a Liberty Bank employee to get your personal information in order to use it fraudulently.
- ☑ Avoid clicking suspicious links and/or responding to emails and texts urging you to act quickly.
- ☑ Never give out account numbers, social security numbers, credit card numbers, PINs, CVVs, passwords, or passphrases.
- ☑ Never trust caller ID: Always validate a person's organization by hanging up and calling them back through the official phone number.
  - Never release information to the caller or the sender of an email.
  - Verify the requestor and the requestor's right and need to know the information.
  - Never rely on the phone number or email address or link they provide; instead look up the contact number listed on your statements, or look up the company's website on the internet to obtain their contact information and then contact them directly.
  - In the case of Liberty Bank, call our Customer Service Center directly at (888) 570-0773. You may also complete the Contact Us form on our web site or send us an email through online banking.
- ☑ Send money to trusted sources only: only send money to friends, family or others you know and trust. Do not buy goods or services from people you are unfamiliar with or have never met.
- ☑ Keep your passwords safe and up-to-date. Create a strong, unique password for each online account you have.
  - Always keep your passwords up-to-date, changing them every so often, and follow the recommended password format (generally a password that includes at least one upper case letter, lower case letter, numbers and symbols).
  - No one should know your passwords other than you.
- ☑ Browse safely; make sure your internet browser is on the latest version and its configuration adheres to security best practices.
- ☑ Protect your devices by ensuring the latest anti-virus and/or spyware software is installed and updated on your device(s), and apply operating system and application updates (patches) regularly.
  - Never use an unsecured network or a shared computer to access your personal or account information.
- ☑ Turn off your computer when not in use.

LIBERTY BANK

Common Red Flags to Look Out For

- ☑ Asking you to purchase gift cards and provide the codes as a form of payment;
- ☑ Instructing you to make a cash deposit for a sweepstakes;
- ☑ Asking you to cash or deposit a check on behalf of someone else;
- ☑ Instructing you to deposit a check received in the mail;
- ☑ Instructing you to cash or deposit a check received in the mail and ask that a portion of the funds be withdrawn and sent to pay taxes & fees; and/or
- ☑ You may be offered more than the price you are asking and receive a request to send the overpayment somewhere you are not familiar with.

Extra Layers of Security to Consider When Banking with Liberty

- ☑ Liberty Bank will NOT request a customers' personal information through email or provide links within an email to update information
- ☑ Liberty Bank employees will NOT ask you for your Online Banking password and we won't request that you send an unsecured email containing your personal or financial information.
- ☑ Download Liberty Bank's Mobile Banking app and "turn on" mobile app alerts.
- ☑ For an extra layer of security when calling Liberty Bank, you can add a passphrase to your profile that only you would know.
- ☑ Regularly review your account activity and credit card statements and report suspicious activity to our Customer Service Center promptly.

Source: Liberty Bank's Operational Risk Management Team

For more information: liberty-bank.com/privacy-and-security