Conducting Your Transactions Online

Federal financial regulators are reporting that Internet threats have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber-criminal groups are increasingly targeting financial institutions, compromising security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

In order to help ensure the security of your online transactions, we want you to know that:

- We will never email, call or otherwise ask you for your user name, password or other electronic banking credentials
- You can help protect yourself by implementing alternative risk control processes like:
  - Making sure you choose an adequate user name and password that, at a minimum, mixes in small case letters, upper case letters and numbers
  - Periodically changing your password (e.g., at least every 90 days)
  - Having current anti-malware and anti-virus software
  - Safeguarding your user name and password information
  - Making sure you have a firewall in place when conducting your financial transactions
  - Logging off the system when you're done conducting business (don't just close the page or "X" out of the system)
  - Monitoring your account activity on a regular basis

In addition, we may require owners of commercial accounts to perform their own risk assessments and controls evaluations. For example:

- Make a list of the risks related to online transactions that your business faces including
  - Passwords being written down and left out in the open
  - The use of old or inadequate passwords
  - The possibility of internal fraud or theft
  - Delays in terminating the rights of former employees
  - The lack of dual control or other checks and balances over individual access to online transaction capabilities
- An evaluation of controls your business uses may include
  - Using password protected software to house passwords in
  - Conducting employee background checks
  - Initiating a policy and process to terminate access for former employees
  - Segregating duties among two or more people so no one person has too much access or control
  - Conducting internal or third party audits of controls
  - Using firewalls to protect from outside intrusion or hackers

Federal regulations provide consumers with some protections for electronic fund transfers. These regulations generally apply to accounts with Internet access. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account. Note, however, that in order to take advantage of these protections, you must act in a timely manner. Make sure you notify us immediately if you believe your access information has been stolen or compromised. Also, review your account activity and periodic statement and promptly report any errors or unauthorized transactions. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on these types of protections. These disclosures are also available online (or ask us and we will gladly provide you with a copy).

If you become aware of suspicious account activity, you should immediately contact the authorities and contact us at the number listed below.

CROSS BANK
399 Merriman Ave E - P.O. Box 9
Wynne, AR 72396-0009
Telephone (870) 238-8171

When you're ahead of the game, you can't be gamed.

10 Ways to Be Cyber-Secure at Home

Identify your perimeter

Less is more! The fewer connected devices and entry points you have, the safer your network is.

Update software and devices regularly

Regular updates make you less vulnerable to attack. Only download updates from the manufacturer and enable auto-updates when possible.

Secure your Wi-Fi network

Routers often have default credentials that people don't know about. Disable the "remote configuration" option in your router and change both your Wi-Fi password and your router password.

Watch out for insecure websites

Always use HTTPS for sensitive communications. Don't ignore browser warnings and always remember to check the website address carefully for misspellings and oddly-placed letters or numbers. When in doubt, manually enter the URL in your browser.

Back up your files

Backups save your information if your device breaks or is taken over by an attacker. Back up files to a removable device that can be locked away safely, such as a CD or flash drive.

Don't download carelessly

Files can contain malware, and websites aren't always what they appear to be. Always verify sender identity before downloading files and remember: If it comes from an oddly-spelled email or is hosted on a site that makes your browser generate a warning, stay away!

Encrypt devices to deter thieves

Encryption renders files unreadable without the correct key. Some devices offer the option to encrypt individual files or the entire device. Consider which solution suits your needs best.

Practice password safety

Choose long passwords containing uncommon words. Use unique passwords for sensitive accounts and a password manager to help you remember them.

Always use antivirus software

Antivirus needs updates, too! Set it to auto-update.

Keep yourself informed

New cybersecurity bugs and attacks pop up every week. Staying informed about the latest threats will help you be safe!

INFOSEC

Learn more at infosecinstitute.com

Identity Theft

What to know, What to do

FEDERAL TRADE COMMISSION

IdentityTheft.gov

Is someone using your personal or financial information to make purchases, get benefits, file taxes, or commit fraud? That's identity theft.

Visit IdentityTheft.gov to report identity theft and get a personal recovery plan.

The site provides detailed advice to help you fix problems caused by identity theft, along with the ability to:

- get a **personal recovery plan** that walks you through each step
- update your plan and track your progress
- print pre-filled letters and forms to send to credit bureaus, businesses, and debt collectors

Go to **IdentityTheft.gov** and click "**Get Started**."

There's detailed advice for **tax**, **medical**, and **child identity theft** – plus over thirty other types of identity theft. No matter what type of identity theft you've experienced, the next page tells you what to do right away. You'll find these steps – and a whole lot more – at **IdentityTheft.gov**.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- ☐ Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.

- ☐ Change logins, passwords, and PINs for your accounts.

Step 2: Place a fraud alert and get your credit reports.

- ☐ To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.

  - **Experian.com/help**
    888-EXPERIAN (888-397-3742)
  - **TransUnion.com/credit-help**
    888-909-8872
  - **Equifax.com/personal/credit-report-services**
    800-685-1111

  Get updates at **IdentityTheft.gov/creditbureaucontacts**.

- ☐ Get your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call 1-877-322-8228.

- ☐ Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 3: Report identity theft to the FTC.

- ☐ Go to **IdentityTheft.gov**, and include as many details as possible.

  Based on the information you enter, **IdentityTheft.gov** will create your Identity Theft Report and recovery plan.

Go to IdentityTheft.gov for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company.

IdentityTheft.gov can help – no matter what your specific identity theft situation is.

FEDERAL TRADE COMMISSION
IdentityTheft.gov
September 2018