Online Banking Security Guarantee

Provided you have met your security responsibilities, if you experience a loss resulting from a transaction through online banking that you did not authorize, we offer an Online Banking Security Guarantee for account losses; however, when a member becomes a victim of fraud, either when a fraudster accessed their account or when they have sent money to a fraudster, whether the Credit Union will reimburse the member for the fraud-related loss depends on how the fraud occurred.

We investigate and assess all fraud situations and, in doing so, determine whether you have complied with the **Account Terms & Conditions Agreement** (this will be a live link to our website). When you signed your Terms & Conditions Agreement, you agreed to be responsible for all account activities and transactions, including any that are fraudulent. Please take a moment to review our updated **Account Terms & Conditions Agreement. (live link)**

If, after investigating the fraud, it is determined that you did not take reasonable actions to protect your account, the credit union is not responsible for your losses.   Common scenarios where you will be held responsible for account losses:

- **Authorized Push Payment (APP) Fraud:** If a scammer tricks you into sending money (e.g., via wire transfer, e-transfer, or bill payment), the credit union considers it authorized by you, even if the authorization was based on pretenses.

- **Security Credential Compromise:** If you share your Member ID, Personal Access Code (PAC) and/or your One-Time Passcode (OTP) with a scammer, or enter them into a fake website, the credit union policy is that you failed to safeguard your personal authentication information.

- **System Validation:** If our system logs show the transaction was initiated from your recognized device, IP address, or that the correct 2FA / OTP was successfully entered, the credit union policy is that we are not responsible for any losses you have incurred.

- **Gross Negligence:** Our terms and conditions hold you responsible if you do not follow basic security practices, such as leaving a logged-in device unattended, failing to install security software, or ignoring warning signs of a scam

Member Security Responsibilities.

To ensure that you are doing your part in protecting yourself from online cybersecurity fraud, you are responsible for ensuring the following*:

- **Protecting your Unique Identifiers:** Do not share your unique personal authentication information. Note that we will never ask for your unique authentication information, including your Personal Access Code (PAC) or your one-time 2FA/OTP, which you received either by text message or to your email.

- **Keep all software up to date:** Make sure to turn on automatic updates in Windows Update to keep Windows, Microsoft Office, and other Microsoft applications up to date. Turn on automatic updates for non-Microsoft software, especially browsers, Adobe Acrobat Reader, and other apps you regularly use. Ensure your cell phone also receives real-time updates by turning on automatic updates.
- **Use antivirus software:** If you run Windows, you have Windows Security or Windows Defender Security Center installed on your device.

- **Password Protection:** Password length is a primary factor in characterizing password strength. To strengthen the security of your online information, ensure your passwords are a random mix of 14 to 16 characters, including letters (upper and lower case), numbers, and special characters. Never write your passwords down; instead, memorize them or use a password manager such as LastPass™.

- **Never Share Online Banking Credentials:** If someone needs to support you with your banking, you can make arrangements with the Credit Union to add them to your account. Formally adding someone to your account, rather than sharing credentials, protects you from liability for fraud and terms-of-service violations.

- **Browse the Web Safely:** Avoid visiting sites that offer potentially illicit content. Many of these sites install malware on the fly or offer downloads that contain malware. Use a modern browser like Microsoft Edge, which can help block malicious websites and prevent malicious code from running on your computer.

- **Never use public WIFI to access Online Banking:** Cybercriminals can use unsecured Wi-Fi networks to spread malware to other devices on the same public network, especially if those devices aren't up to date. They can also intercept data transmissions and trick users into revealing sensitive credentials, such as your online banking details.

- **Stay Away from Pirated Material:** Avoid streaming or downloading movies, music, books, or applications that do not come from trusted sources. They may contain malware.

You must promptly, within 24-hours, report any financial losses that you believe result from cybercrime to the Credit Union for us to investigate and assess the incident.

*This list of safeguards is not exhaustive and does not cover all potential risks. Additional measures may be required depending on your specific circumstances