AMPLIFY CREDIT UNION

ONLINE BANKING SECURITY POLICY

AMPLIFY is committed to offering its members accessible and secure electronic access to its banking products and services. For this purpose, Amplify utilizes safety protocols to safeguard the confidentiality and integrity of the personal and financial information managed. These protective measures cover the entire interaction between the member and AMPLIFY, from the beginning of the session to its conclusion. Security encompasses, but is not limited to, the following:

ONLINE AND MOBILE BANKING SERVICES ENROLLMENT AND USE

Members can Enroll in Online and Mobile Banking Services at www.goamplify.com or contact us for assistance. Users can access AMPLIFY's Online Banking at www.goamplify.com or download our app from the Apple App Store or Google Play Store. The Mobile Service is compatible with devices that support a mobile browser. To perform transactions, users must enter their Login ID and Password. New Passwords must be changed upon first login. Users can enable biometric options (Fingerprint, Facial Recognition) under security preferences after initial setup. Biometric availability depends on the device. If users forget their password, they should use the Forgot Password feature on our website or in the mobile app. Passwords require a set number of characters, including one upper-case letter, one special character, and one number. Further details will be provided during enrollment.

SECURITY GUIDELINES

Security measures aim to safeguard the privacy and integrity of personal and financial data throughout the user's session with AMPLIFY, from start to finish, rather than detecting errors.

Practices and Procedures

- Account Security: Login IDs are locked after multiple failed login attempts. To reactivate your password, contact AMPLIFY in person or by phone.
- Password Management: Change your password periodically for security. Reusing old passwords is not allowed.
- Session Timeouts: The service will automatically logout after a period of inactivity, prompting you to restart the session.
- Confidential Information: AMPLIFY never requests updates for confidential information like passwords or social security numbers.
- Monitoring and Vigilance: Regular monitoring is conducted to detect attempted attacks.
- Digital Security: AMPLIFY uses Digital Certificates for authentication and encryption of electronic transactions, indicated by a closed padlock icon and a URL starting with "https."
- User Identity Validation: Additional elements verify users' identities to maintain confidentiality and data integrity.
- Access Protocols: AMPLIFY reserves the right to block, limit, or restrict access to users providing false information, posing risks, or abusing privileges.

Responsibility of Users of Online and Mobile Banking

- Use a strong password that only you know, avoiding names, key dates, or phone numbers.
- Protect your device with up-to-date antivirus software to counter malicious programs.
- Protect your password by keeping it private; avoid writing it down or storing it insecurely, and never share your login information. Refrain from saving passwords on devices to prevent potential security breaches.
- Change your password immediately if you suspect exposure or after 30 days of inactivity.
- You're responsible for safeguarding online banking information. Sharing it grants others access to your accounts and transactions, allowing them to review account details, access services, and make transfers.

ACCESS AND MAINTENANCE

Services are available 24/7, with the exception of scheduled maintenance periods. Access may be modified, suspended, or terminated at any time without notice. We are not responsible for any fees resulting from such access restrictions or failures due to system issues or unforeseen events. The Credit Union can change this Agreement's terms or any Service Section in line with service updates or legal requirements. Using Online Banking Services after changes take effect indicates your agreement with them.

ACCESS DEVICES, BROWSER ACCESS, AND INTERNET SERVICES

To use Online Banking Services, you need your own Internet-capable Access Device and related equipment (the "Hardware"). You are responsible for purchasing, installing, operating, and maintaining the Hardware, Software, and Internet service, along with any associated costs, including virus protection. The Credit Union is not liable for service issues caused by incompatible or improperly maintained hardware and software. They may update or replace software without notice provided this does not substantially affect services or alter obligations. Browser compatibility may change over time:

Supported browsers (current and previous two major versions): Google Chrome (recommended), Mozilla Firefox, Microsoft Edge (Windows only), Apple Safari (Mac OS only). Please note that while browsers not listed may still function, users may encounter issues. We strongly recommend using a supported browser to ensure an optimal experience and to prevent any potential problems.