Members United CU
Mobile Banking Policy

Having acknowledged that technology is the driving force of the future, offering this convenience makes us attractive and produces growth. The decision to offer Mobile Banking was made several years ago in the response to member request. Our due diligence and planning process included, but was not limited to, the following activities:

- The credit union evaluated our member's expectations and demands.
- The credit union evaluated internal and external expertise and resource requirements to support a Mobile banking system.
- The credit union assessed the risks and required controls, particularly those related to system security.
- The credit union developed effective policies and procedures that cover the program.
- The credit union developed a training/marketing program to educate the staff, board and members.

Security is a critical issue. Our goal is to distribute our products and services in a safe, accurate, efficient and convenient manner. Cusa/Fiserv was chosen as our mobile partner based in part on the working relationship we have had for the last twenty years. We are confident in their ability to supply, meet and protect our needs. We are familiar with the company assets and feel confident that this organization will be here to provide our future requirements as we continue to grow and as technology continues to evolve.

The board recognizes that Mobile banking activities involve a wide range of potential risks. Some of these are unique to this new delivery channel, while others represent general concerns that are common to traditional banking practices.

MULTI-FACTOR AUTHENTICATION

Because we are committed to ensuring the account is secure, we've structured enhanced security to prevent unauthorized access in three important ways:

1. Enhanced security displays an image and personal phrase (chosen by the member) during login so the member can confirm that they are accessing their credit union's valid website rather than an imposter.
2. Enhanced security allows the member to register their mobile device to help us recognize their device during login.
3. Must complete the 6-step enrollment process through Virtual Branch to be able to use the mobile banking product.

SECURITY

To achieve an adequate level of security at the onset, Virtual Branch applications are opened and made operational by staff that has been trained regarding privacy measures. Members are

assigned a temporary pin and encouraged orally and in writing to change this pin immediately and often to protect their privacy. Login attempts are also limited for further protection.

Cusa/Fiserv has developed extensive security and disaster recovery policies. Company passwords, firewall servers and secure encryption for information transmissions between the member, company and credit union are common features.

LEGAL FRAMEWORK

It is the policy of this credit union to comply with all electronic commerce laws and the laws of the state of Georgia.

No computer system, regardless of security measures, is invulnerable to attack and no member/credit union relationship is perfect at all times. Therefore, we have included language on our applications to express our position regarding any member dispute. Recognizing that our credit union was chartered in the state of Georgia, to do business in the state of Georgia, we have asked each member to sign an agreement that any dispute will be settled in the state of Georgia according to Georgia laws.

Established 8/16