Online & Mobile Banking – Security Overview

Login ID's and Passwords:

The use of TINs, SSNs, account numbers, or other personally identifiable information (PII) should not be used when creating account credentials. Additionally, the use of email addresses as account credentials is generally discouraged. Password requirements meet general criteria – minimum 8 (alpha/numeric) characters.

- You should select a unique login ID that does not contain sensitive information, which may be compromised in the event of those credentials being stolen.
- You should choose a login ID that would not easily be guessed, or that would not likely be very similar to another customer's login (Fred, Fred1, etc.)

Secure Access Codes (SACs):

Secure access codes are randomly generated codes that you are prompted to enter during the following events:

- initial login process
- subsequent logins, if your browser or device has not been previously registered
- transaction approval process, if the transaction type and amount require code-enabled authorization
- password reset process

SACs can be delivered through automated voice call or SMS message. Permitting only out-of-band (OOB) delivery through channels such as SMS or voice provides a more secure method of delivery for SACs and reduces the likelihood of the SAC being maliciously intercepted. The expiration time period for a SAC code is 10 minutes.

Note: SACs should never be shared across users, and they should never be setup for delivery to a non-dedicated number, such as main phone number of a business, where someone other than the customer could answer the call.

Browser Registration (Cookies):

Browser registration offers you the ability to register your browser upon login, after successful authentication utilizing account credentials, and a one-time secure access code (SAC). When you register your browser, that browser is issued an HTTP cookie or Flash Shared Object (FSO), which is authenticated by the online banking server at each subsequent login from that browser. This feature is referred to as simple device authentication.

Note: You should only register browsers on your personal computer. Never register a browser on a public or shared device.

Session Timeout:

A sliding session timeout will take effect after 15 minutes of inactivity. The session can be extended by pressing "OK" when the warning is presented.

A lifetime session timeout will take effect after 45 minutes, regardless of activity.