



FFIEC guidelines require multiple levels of authentication for consumers using electronic banking. The Q² solution is referred to as “Multifactor”. This process employs the use of email and/or voice delivery of a temporary access code to satisfy the requirements of a user both “knowing” and “having” the data elements necessary for authorized access to online banking.

Secure Access Code Delivery

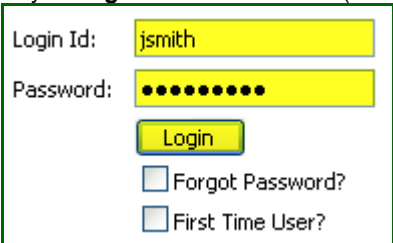
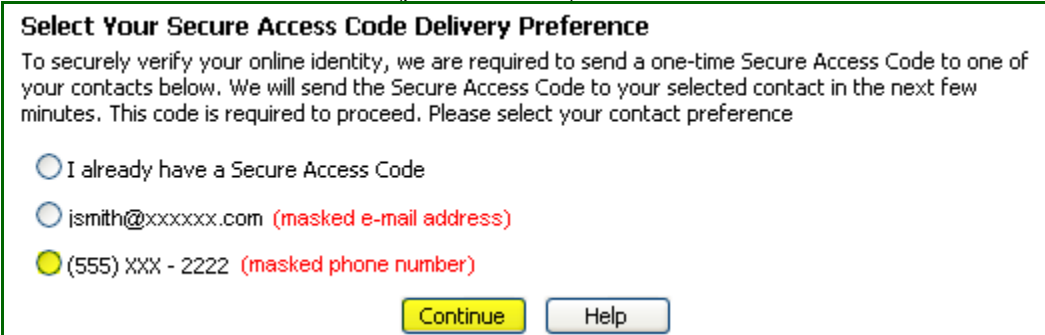

Via Telephone:

- Secure Access Codes are never left on voice mail.
- Secure Access Codes are only used in combination with the requesting customer’s User ID and Password.
- Unused Secure Access Codes expire after 20 minutes.
- Used Secure Access Codes immediately expire and cannot be reused.
- If the user believes the Secure Access Code request is fraudulent, they are presented with the option to immediately disable their online and/or voice account access.

Via E-mail delivery:



- “From” address is set by the financial institution to restrict replies or forwarding.
- Secure Access Codes are only used in combination with the requesting customer’s User ID and Password.
- Unused Secure Access Codes expire after 20 minutes.
- Used Secure Access Codes immediately expire and cannot be reused.

Login Steps Utilizing Multifactor (for users that have previously logged in)

| Step | Action |
|---|---|
| 1 | Key in Login Id and Password (1 st factor – something you know) click Login  |
| 2 | Select Secure Access Code Delivery Preference A listing appears with the user’s partial or masked contact information - the user chooses the delivery method for their secure access code (phone or e-mail)  |
| 3 | The voice server initiates the outbound call to the user’s phone or an outbound e-mail to the user’s e-mail address (the phone number or e-mail address must reside in the banks system as the user’s Secure Access Delivery method) |
|  | Upon answering the phone or viewing the e-mail, the user hears/sees a generic message from the bank indicating they have requested a temporary access code (the message does not indicate that the call/e-mail is for Online banking, Voice, ATM etc. - the user should be expecting the call/e-mail) |



Login Steps Continued

| Step | Action |
|---|---|
| 4 | <p>Key in the Secure Access Code received by phone/e-mail (2nd factor – something you have)</p> <div style="border: 1px solid green; padding: 5px;"> <p>Enter Delivered Secure Access Code</p> <p>Once you receive your Secure Access Code, enter it below.</p> <p>Secure Access Code * <input style="background-color: yellow;" type="text" value="543889"/></p> <p style="text-align: right;"> <input type="button" value="Continue"/> <input type="button" value="Help"/> </p> </div> |
|  | <p>The Secure Access Code is valid for 20 minutes</p> |
| 5 | <p>Click Continue</p> <p>Activate Browser: choose one of the following options: Activate this computer for later use – a logical option for a home or work computer OR Give me one-time access only (do not activate this computer) – a logical option when using a public PC (at a hotel, in a library etc.)</p> <div style="border: 1px solid green; padding: 5px;"> <p>Activate Browser</p> <p>Are you at a private computer that you will use regularly to access online banking? If so, we can activate your browser for future access. If you are at a public computer, select "One Time Access" below and this computer will not be activated.</p> <p> <input checked="" type="radio"/> Activate this computer for later use <input type="radio"/> Give me one-time access only (do not activate this computer) </p> <p style="text-align: right;"> <input type="button" value="Continue"/> <input type="button" value="Help"/> </p> </div> |
|  | <p>A secure access token is placed on the computer in the form of a "cookie" – if the cookie is deleted, this registration process must be repeated</p> |
| 6 | <p>Click Continue</p> |