



## OUT-OF-BAND AUTHENTICATION FAQs

### 1. What is Out-of-Band Authentication?

Out-of-band Authentication (OOBA) is a simplified way of securely accessing your account online. Text messaging or phone calls are used to confirm an account holder's identity. Through this form of identity verification, you are better protected from fraudulent online attacks. If someone other than the account holder attempts to use invalid information, the account will become locked and available for access only by calling an ASI Member Service Representative.

### 2. How does this affect my online banking activity?

If you use a desktop or laptop to access your online banking account, you can now receive a unique, four-digit verification code to confirm your identity. You will no longer be required to answer security questions. Simply verify the land-based or cell phone numbers for the account, and we will send you a code allowing access to your information.

### 3. What if I change my phone number, or my correct number is not listed on my account?

We urge all members to update their contact information as soon as possible after a change. If we do not have your correct phone numbers, you will not receive a code via text or phone call. We can only contact you at the phone number on file. If you wish to verify the accuracy of your contact information, [visit any branch](#), or contact us at 504.733.7274, or 800.749.6193.

### 4. I use the ASI mobile app to access my banking information. Does OOBA affect me?

Members who utilize our Mobile Banking app will not experience a change in logging into their account. Security questions will remain active and will continue to provide you with top-level security from online threats.

### 5. What should I expect when logging into Online Banking once OOBA is implemented?

After inputting your username, if we don't recognize your device or network, you will receive a security message to **Continue with Security Code**. Click to continue.

- When logging into Online Banking from a desktop or laptop computer, after inputting your username, if we don't recognize your device or network, you will receive a security message to **Continue with Security Code**. Click to continue.
- The security code can be delivered to you by phone call or text message. The contact information displayed on the screen is currently on file with ASI. You may select how you want to be contacted.
- If you select to receive a phone call, you will receive your unique security code via automated messaging. You will enter your code on the current screen to access Online Banking.
- If you choose text message, click Continue and you will be sent a one-time security code that will be sent to your mobile device.

**6. Do I need to keep the security code given to me for future logins?**

The security code is a unique, one-time code and cannot be used again. Each time your online identity cannot be identified at login, a new one-time security code is required.

**7. How long do I have to wait for a phone call or text message?**

You should receive a code within seconds of completing the request. If you do not, click on **“I didn’t receive a code”** link on the screen for help.

**8. What if I do not receive a text message?**

If you do not receive a text message within 60 seconds, please select the “receive a phone call” option in the dialog box. You will receive an automated phone call with your unique code.

**9. Why can’t I receive my security code by email?**

Federal Financial Institutions Examination Council (FFIEC) guidelines state that you must be contacted through a different channel than you are currently using to access Online Banking.

**10. How much time do I have to complete my authentication?**

If you do not validate your identity with the one-time security code within 3 minutes, you will be directed back to the Online Banking login screen.

**11. Why isn’t my username and password enough to identify me?**

Your username and password can be easily obtained through malicious software that may be unknowingly installed on your computer. Any change in how you access Online Banking (different computer, different geographic location), signals us to request additional verification.

**12. Why am I asked to authenticate when I am using the same computer from the same location I always access Online Banking?**

This is generally due to a change made to your computer that prevented its identification. Changes that would alert our system:

- Browser updates
- Browser setting changes
- Clearing cookies
- Computer date out of sync with actual date
- A single user using many devices in a short period of time
- Multiple users using the same device in a short period of time

**13. What if I use multiple devices to access Online Banking?**

If you use the same devices on a regular basis, the device profiles are recognized by Online Banking.

**14. What if I use public computers to access Online Banking?**

Online Banking is a gateway to vital account information. Every computer or device you use should provide security protection from unauthorized access. For this reason, we strongly advise against logging in from a computer if you do not know the reliability of its virus protection and firewalls.

**Helpful Tips**

- Add **ASIFCU.ORG** to your trusted sites.
- If using Internet Explorer as your browser, make sure “Preserve Favorite Sites” is not checked.
- Clear the cookies on the device.

**Still have questions?**

If you still have questions about OOBA, you may speak to a Member Service Representative at [504.733.7274](tel:504.733.7274), or [800.749.6193](tel:800.749.6193).