ROOBA

(Regions Out-of-Band Authentication)

Frequently Asked Questions:

At Regions, our priority is the safety of our clients' financial information. As services are integrated with the Regions OnePass commercial online portal, several security enhancements using ROOBA SM (Regions Out-of-Band Authentication) are being implemented. Out-of-band authentication is a secure tool for multifactor authentication. The Regions OnePass online services portal uses out-of-band authentication to provide an additional layer of security. For example, ROOBA is used to verify the identity of OnePass users who have administrative access due to the ability to create and modify user permissions. ROOBA is also used for security authentication at the point of ACH and Wire release.

- ROOBA provides enhanced security against the potential dangers in your PC or network to verify your identity.

- The ROOBA verification process requires a security code to be entered using a telephone when a ROOBA user verification challenge is received. The phone provides a secondary means of authentication using an "out-of-band" authentication channel.

Please review the following information to help address any questions you may have.

I. What is Out-of-Band Technology and ROOBA Authentication?

- ROOBA is an authentication method through which the user validates and/or acknowledges certain application events using their mobile or landline phone, rendering some of the most common online fraud attacks ineffective (i.e., man in the browser, man in the middle, and key logging). For example, ROOBA is used to verify identity for security when releasing transactions through iTreasury, such as those initiated by ACH or Wire.

- ROOBA replaces security tokens for applications that require them and provides added security against fraudulent attempts. A rash of prominent security token breaches has brought new attention to an increase in the frequency and sophistication of computer hacking that ROOBA technology can help mitigate or prevent. Out-of-band authentication technology takes the authentication out of the browser to eliminate this vulnerability by better safeguarding against man in the browser attacks.

II. How does ROOBA security compare to security tokens?

- ROOBA circumvents the potential dangers in the PC or network to verify your identity by using phone authentication.

    - Out-of-Band Authentication uses a "channel" or "communication path" that is not directly associated with the access path to verify the authenticity of your device (PC). This is referred to as "Step-up Authentication."

    - The "Step-up" process requires you to have a phone in which to enter a code to respond to the ROOBA prompt.

- ROOBA provides added security because even if a fraudulent user gains all security credentials to your online banking account, a transaction cannot be completed without access to the second authentication network (your phone).

III. What are the benefits of Out-of-Band Authentication?

- ROOBA provides the most secure method of safeguarding our clients' information and their accounts. Should a fraudster gain access to your user credentials, he would be unable to complete a transaction not having access to the secondary authentication path you have chosen; for example, your mobile phone or landline, thus making ROOBA an additional layer of enhanced security.

- ROOBA also provides a more streamlined log-in process for online applications by providing one access portal and by eliminating the need for security tokens for applications that previously required their use.

IV. How do I set up ROOBA and how will phone authentication work?

While creating their OnePass profile, users are asked to enter a primary and secondary phone number, elect a communication method (Automated Call or SMS/Text), and establish their own four-digit Security Code. When the user engages in a predefined event, such as accessing the Admin Console, the system will give the option of communicating to either phone number enrolled via the method selected (voice or SMS/Text).

- The message delivered will depend on the event being authenticated, will contain details about the event, and will provide the user instructions on how to respond to either accept or reject the event.

- The user would then respond accordingly, utilizing their Security Code per the instructions included in the message delivered.

- In the event the system does not receive the appropriate, affirmative response, the user initiated event will be cancelled.

V. What if my telephone system requires an extension to transfer the call? Will I be able to receive the call from ROOBA?

Yes. If you have an automated system that directs calls, enter an extension beside the phone number(s) you set up in your user profile. When ROOBA calls the telephone number, the call will be transferred to your extension.

VI. What events trigger a ROOBA verification call?

Users who are designated as Administrators, or those with designated access to administration functionality, will be required to use ROOBA when accessing the Admin Console within OnePass. Users who release ACH or Wire transactions will also be required to use ROOBA. Users may also be authenticated when calling Regions Client Services as needed to verify their identity.

VII. What happens if I need to change my telephone number(s) or Security Code?

After you securely establish your OnePass User Profile, which includes your telephone numbers and Security Code for ROOBA, you can update the primary and secondary number designation, as well as the preferred delivery method for each number (Automated Call, SMS/Text) through the My Profile page in OnePass. Additionally, your OnePass system administrator can update your actual phone numbers through the Admin Console.

You may reset your Security Code by selecting that option on the My Profile page and providing your existing Security Code. Your Administrator or Regions Client Services can reset your Security Code through the Admin Console, if you forget your old one.

VIII. How often will I need to change my password in OnePass?

Your password will need to be changed every 60 days. You will receive a prompt to do so.

IX. If I need to work from home or another location, will I still be able to access OnePass?

Yes. The security in OnePass will allow you to simply respond to a ROOBA challenge if it detects any unusual pattern of behavior. You should also enter a secondary phone number to which you will have access, such as a mobile phone, for ROOBA.

Still have questions?

If you still have questions about ROOBA, please contact your Treasury Management Officer. Also see the OnePass Frequently Asked Questions, OnePass User Guide that are available on regions.com/MyOnePass.