

ACI PAYMENTS INC: ADDING MULTI-FACTOR AUTHENTICATION (MFA) TO MY ACCOUNT - FAQ

This document addresses frequently asked questions (FAQ) about adding MFA for My Account users.

What is multi-factor authentication (MFA)?

MFA requires users to provide two or more verification factors to gain access to their accounts. For My Account users, these factors will be their login credentials, meaning their username and password, and a 6-digit time-based one-time passcode (TOTP) provided via text or email.

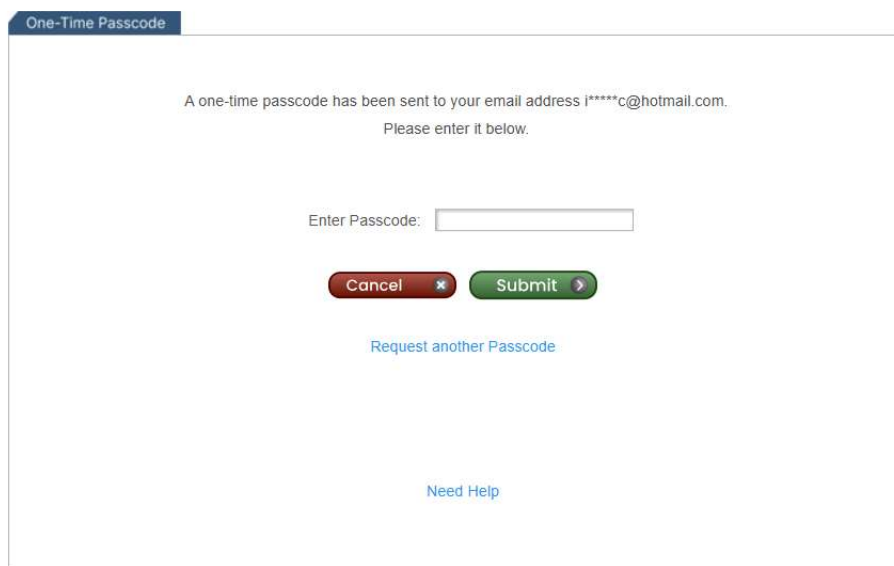
Why is MFA being added to the My Account login process?

To comply with the Gramm-Leach-Bliley Act (GLBA), ACI will enable (MFA) for all our consumer portal logins. The GLBA mandates that financial institutions protect the security, confidentiality, and integrity of customer and consumer information. One key requirement under the GLBA's Safeguards Rule is to implement strong access controls, including MFA.

How will My Account users receive the passcode?

The passcode is a 6-digit numerical code that My Account users will receive either via SMS text to their mobile device or the email address associated with their account.

When My Account users log in with their username and password, they will be prompted to authenticate themselves with a one-time passcode:



The screenshot shows a web interface for entering a one-time passcode. At the top, there is a blue header with the text "One-Time Passcode". Below this, a message states: "A one-time passcode has been sent to your email address j*****c@hotmail.com. Please enter it below." There is a text input field labeled "Enter Passcode:". Below the input field are two buttons: a red "Cancel" button with a white asterisk icon and a green "Submit" button with a white right-pointing arrow icon. Below the buttons is a blue link that says "Request another Passcode". At the bottom of the form is another blue link that says "Need Help".

An email notification with the one-time passcode will be sent to the same email address used to log in. The passcode is valid for 10 minutes. If it expires, the My Account user has the option to request another passcode.

From: do-not-reply@mfa.aciworldwide.com
Date: January 1, 2025 at 3:42:24 PM EST
To: JohnDoe@hotmail.com
Subject: Your OTP Code
Reply-To: do-not-reply@mfa.aciworldwide.com

Dear Customer, Your one-time passcode for secure login is: 731479. You can use this to access your My Account. Please do not reply.

Can My Account users receive their passcode via text?

Yes. If a My Account user has saved a mobile number to their account **prior** to requesting a passcode, they may receive the passcode via text. Otherwise, the passcode will be sent to the email address associated with their account.

Can my organization opt out of having MFA turned on for My Account?

No. MFA is a compliance requirement for our consumer portals. ACI must protect consumer data and comply with governmental regulations.

Why are some My Account users reporting that they cannot access their account after entering their 6-digit code?

A user may be denied access to My Account for one of the following reasons:

- **They wait too long to enter the time-based one-time passcode.** The passcode expires after 10 minutes. If the time has been exceeded, the My Account user will be denied access and must request a new code.
- **They enter the code incorrectly too many times.** If the My Account user enters the wrong passcode six times in succession, they will be denied access for 30 minutes. After 30 minutes, they can request a new code.

What should My Account users do if they continue to have trouble accessing the portal and do not believe they are entering the wrong code?

Once the My Account user has entered the passcode six times in succession, they will be denied access for 30 minutes. After 30 minutes, they can request a new code.