Multi-Factor Authentication (MFA) for the Fraud and Risk Center (FRC)

DISCOVER
Global Network

Frequently Asked Questions & Step-by-Step Guide

Overview:

To enhance security and protect accounts, Discover® Global Network is implementing Multi-Factor Authentication (MFA) for the Fraud and Risk Center (FRC). This additional security layer helps prevent unauthorized access.

Why Is Discover Implementing MFA?

Enhanced Security: MFA adds an extra layer of protection beyond just a password. Even if a password is compromised, unauthorized users cannot access your account without the second authentication factor.

Compliance and Regulatory Requirements: Many industries now require MFA to meet security and data protection standards. Implementing MFA helps Discover® comply with best practices and regulatory guidelines.

Protection Against Cyber Threats: Phishing attacks, credential stuffing, and brute-force attacks are increasingly common. MFA can help reduce the risk of account takeovers.

Strengthened Customer Trust: Discover prioritizes customer trust and is committed to data protection.

Publication Date: 3/6/2025
Internal and External Use Permitted

©2025 DFS Services LLC

Frequently Asked Questions (FAQs):

Q | What is Multi-Factor Authentication (MFA)?

A | MFA is a security measure that requires users to verify their identity using two or more authentication factors.

Q | How Will MFA Affect My Login Process?

A | When logging in, you will enter your Log In ID and Password as usual. You will then be required to verify your identity by entering a temporary identification code sent to the email address registered to your account.

Q | What Authentication Methods Will Be Available?

A | Email is the only MFA method currently supported.

Q | Do I Have to Set Up MFA Every Time I Log In?

A | No, there is no enrollment required, but Users will be prompted with a One Time Password (OTP) prompt upon every login. For each login to FRC, a User will be prompted with the OTP screen, and an email will be automatically sent to the email on file with authorization to log in.

Q | Can I opt Out of MFA?

A | No, MFA is mandatory for all Users to enhance security. This policy is in place to protect your account and sensitive data.

Q | Do I need to set MFA up?

A | No setup is required.

Q | Will I Need MFA for Every Action in the Fraud and Risk Center (FRC)?

A | MFA will be required at login after correctly submitting your username and password.

Q | Who Can I Contact for Help?

A | If you experience any complications with MFA login, please contact the support team at NetworkFraud@discover.com.

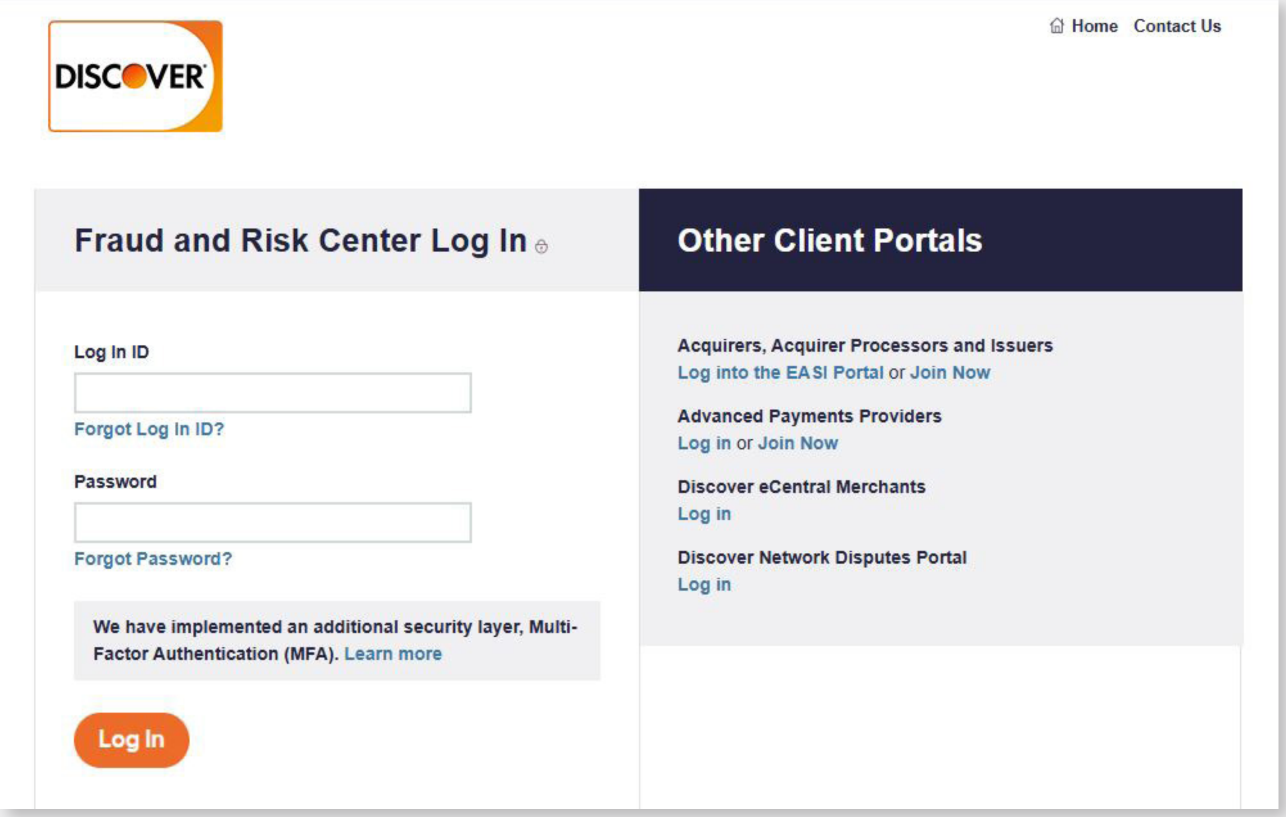
©2025 DFS Services LLC

Step-By-Step Instructions:

The below guide provides step-by-step instructions for enabling MFA on the Fraud and Risk Center. Please review each step carefully and complete the setup as instructed.

If you experience any complications with MFA login, please contact the support team at NetworkFraud@discover.com.

1. **User enters their credentials on the Log In screen.**



Fraud and Risk Center Log In

Log In ID

Forgot Log In ID?

Password

Forgot Password?

We have implemented an additional security layer, Multi-Factor Authentication (MFA). Learn more

Other Client Portals

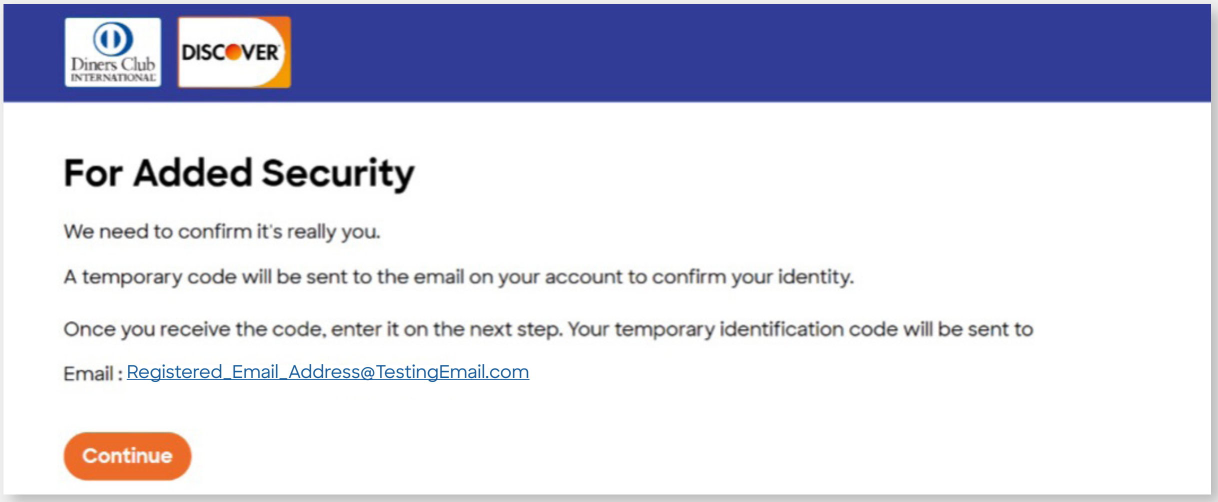
Acquirers, Acquirer Processors and Issuers
Log into the EASI Portal or Join Now

Advanced Payments Providers
Log in or Join Now

Discover eCentral Merchants
Log in

Discover Network Disputes Portal
Log in

2. **After successfully entering credentials, the User will be redirected to the below screen. Upon selecting “*Continue*”, the User will receive an email to the registered email address with a One-Time Password (OTP).**



For Added Security

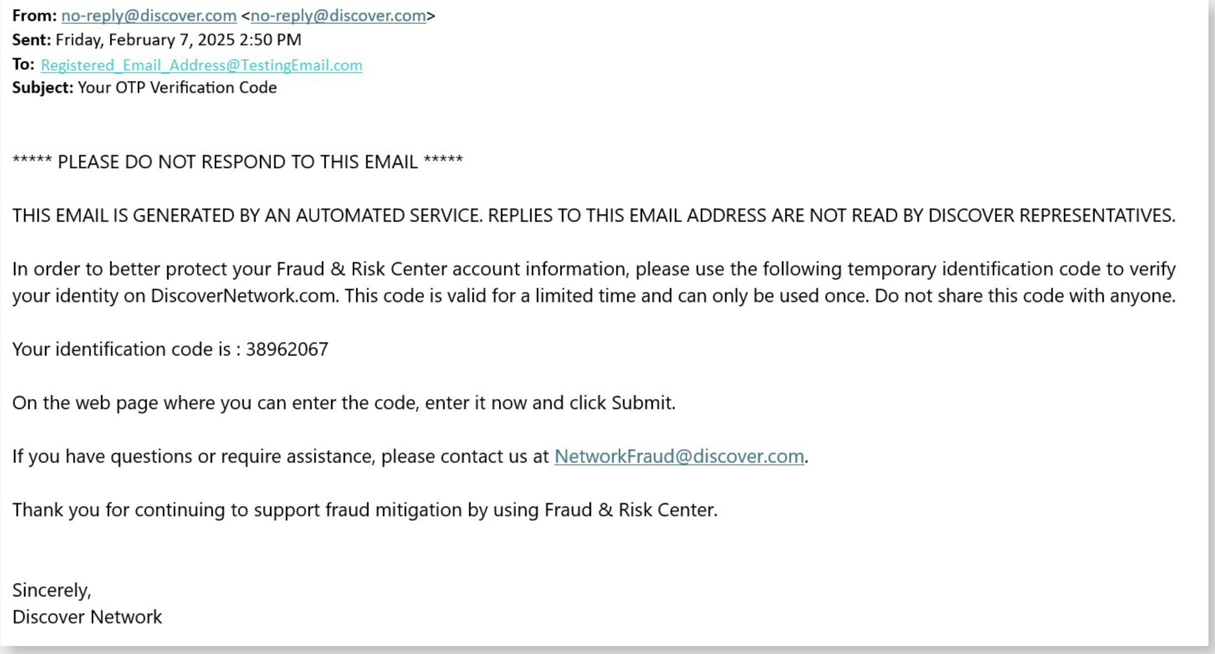
We need to confirm it's really you.

A temporary code will be sent to the email on your account to confirm your identity.

Once you receive the code, enter it on the next step. Your temporary identification code will be sent to

Email : Registered_Email_Address@TestingEmail.com

a. ***The following screen represents the email the User will receive with the OTP.***



From: no-reply@discover.com <no-reply@discover.com>
Sent: Friday, February 7, 2025 2:50 PM
To: Registered_Email_Address@TestingEmail.com
Subject: Your OTP Verification Code

***** PLEASE DO NOT RESPOND TO THIS EMAIL *****

THIS EMAIL IS GENERATED BY AN AUTOMATED SERVICE. REPLIES TO THIS EMAIL ADDRESS ARE NOT READ BY DISCOVER REPRESENTATIVES.

In order to better protect your Fraud & Risk Center account information, please use the following temporary identification code to verify your identity on DiscoverNetwork.com. This code is valid for a limited time and can only be used once. Do not share this code with anyone.

Your identification code is : 38962067

On the web page where you can enter the code, enter it now and click Submit.

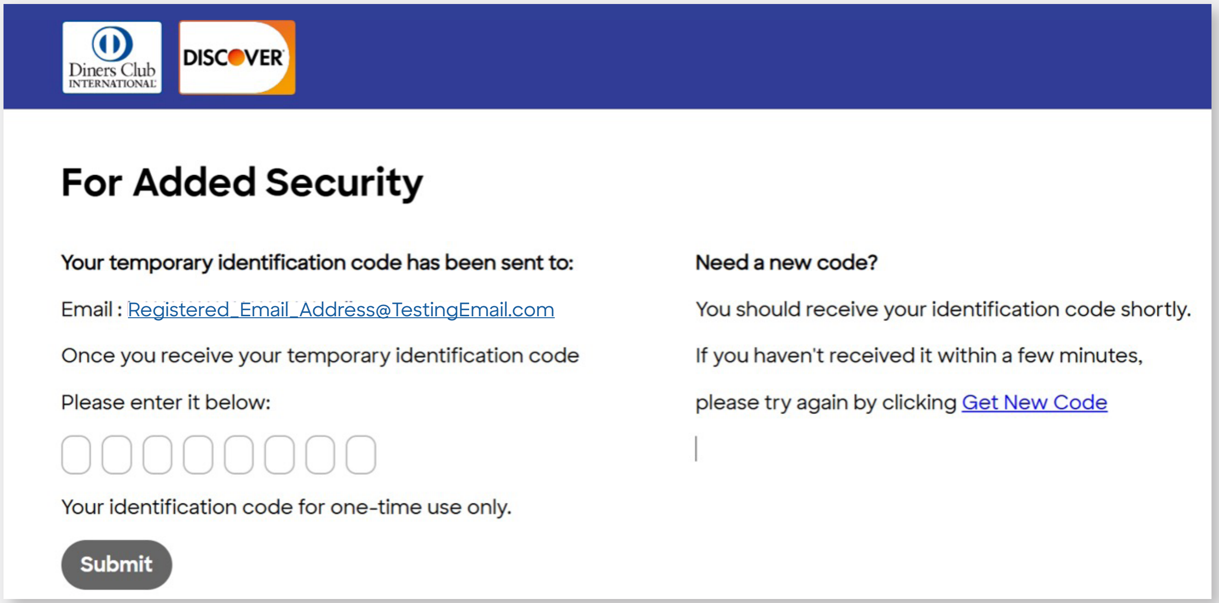
If you have questions or require assistance, please contact us at NetworkFraud@discover.com.

Thank you for continuing to support fraud mitigation by using Fraud & Risk Center.

Sincerely,
Discover Network

©2025 DFS Services LLC

3. Upon receipt of the above email, the User should navigate back to the web browser to the below page. The *"Submit"* button will remain greyed out until the OTP is populated.



For Added Security

Your temporary identification code has been sent to:

Email : Registered_Email_Address@TestingEmail.com

Once you receive your temporary identification code

Please enter it below:

□ □ □ □ □ □ □ □

Your identification code for one-time use only.

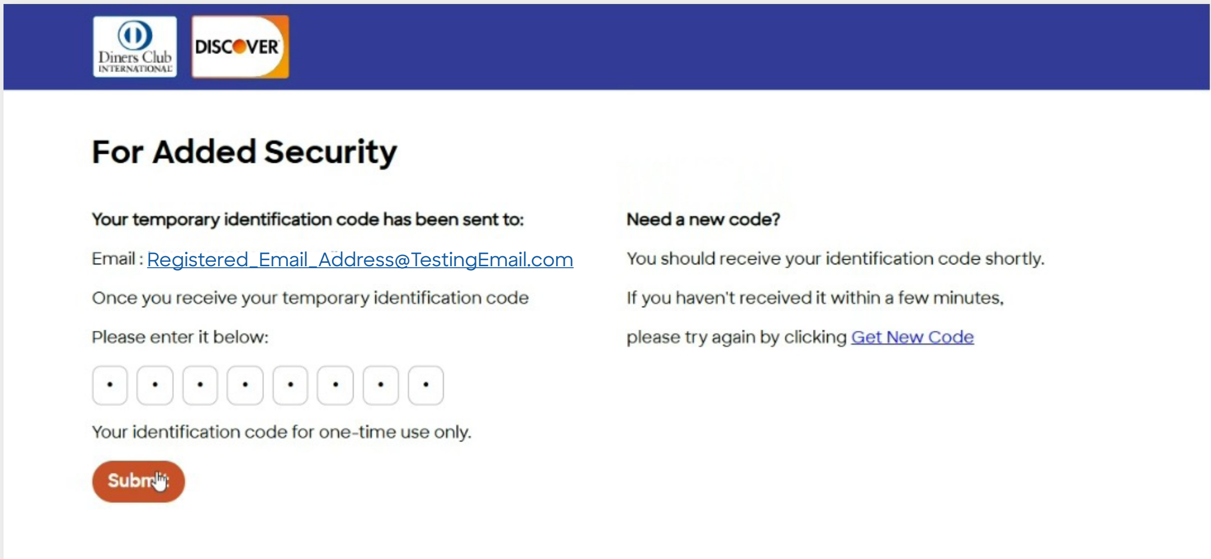
Need a new code?

You should receive your identification code shortly.

If you haven't received it within a few minutes,

please try again by clicking Get New Code

4. Once the User populates the Temporary Identification Code, the *"Submit"* button is enabled and will be highlighted in orange.



For Added Security

Your temporary identification code has been sent to:

Email : Registered_Email_Address@TestingEmail.com

Once you receive your temporary identification code

Please enter it below:

• • • • • • • •

Your identification code for one-time use only.

Need a new code?

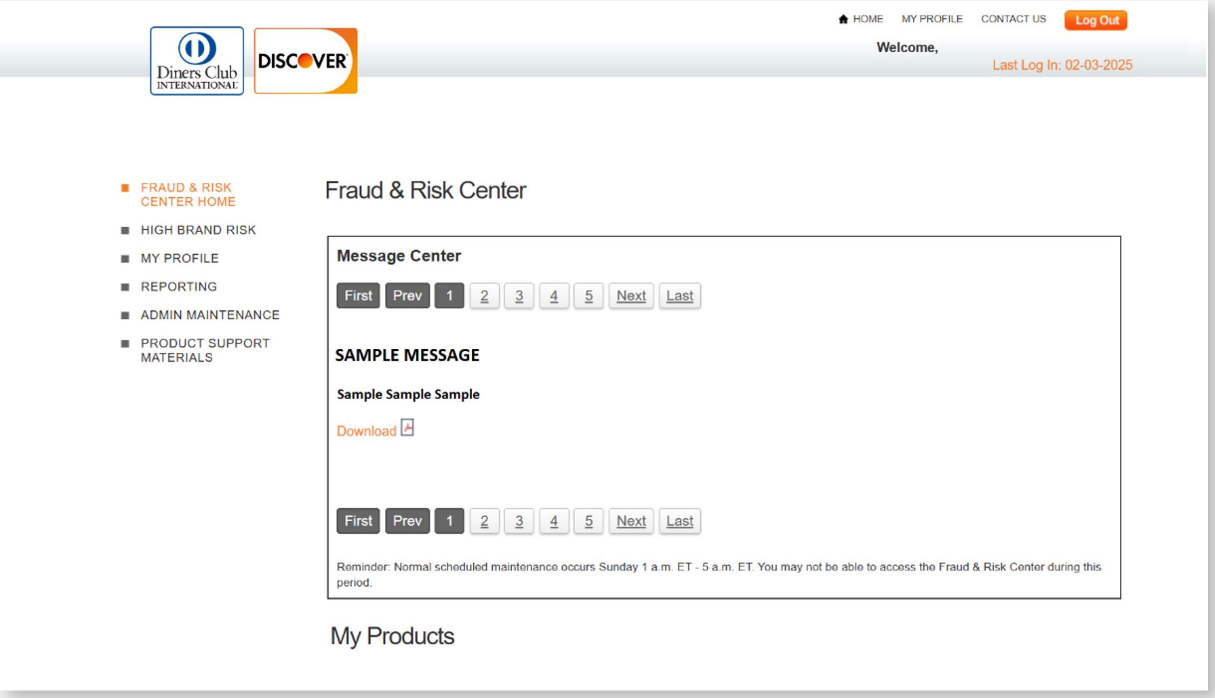
You should receive your identification code shortly.

If you haven't received it within a few minutes,

please try again by clicking Get New Code

©2025 DFS Services LLC

5. **Completion: If the User enters the correct OTP, the User will be redirected to the Fraud and Risk Center homepage, where they can access the product.**



Fraud & Risk Center

Message Center

SAMPLE MESSAGE

Sample Sample Sample

Download

Reminder: Normal scheduled maintenance occurs Sunday 1 a.m. ET - 5 a.m. ET. You may not be able to access the Fraud & Risk Center during this period.

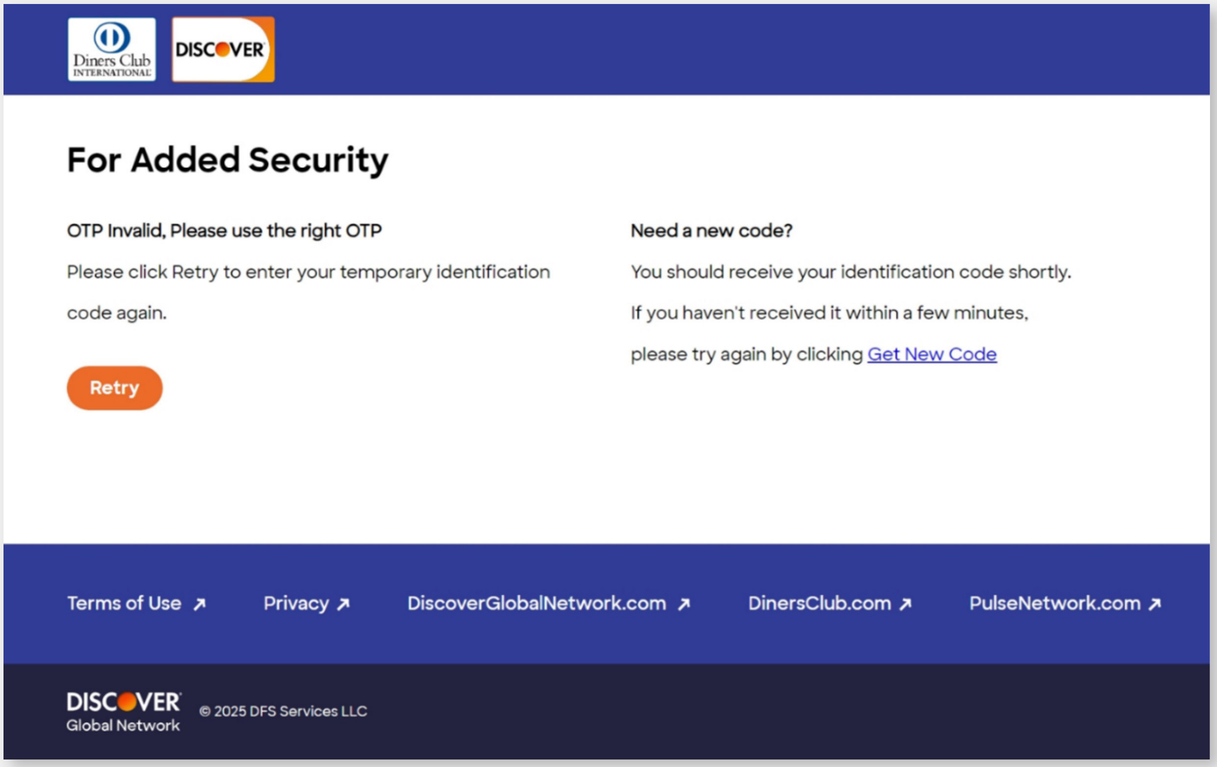
My Products

If the User was not re-directed to the Fraud and Risk Center, there was an error in the process. The below instructions provide additional steps Users can take to resolve the issue. If there are still complications with MFA login after troubleshooting with the below, please contact the support team at NetworkFraud@discover.com.

©2025 DFS Services LLC

There are several reasons why MFA set-up could have been unsuccessful:

1. **The User could have input the incorrect OTP. Please ensure the code is entered exactly as stated in the email received. The User has the option to either select *"Retry"* and input the same code, or request a new code by selecting *"Get New Code"*.**



For Added Security

OTP Invalid, Please use the right OTP

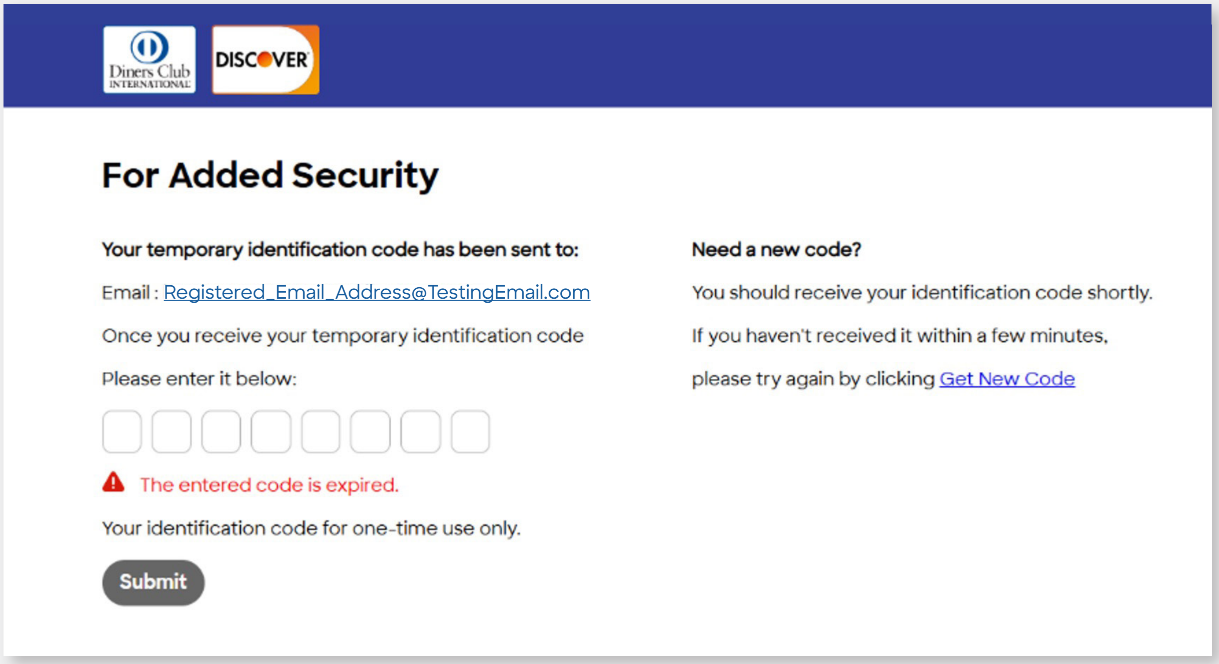
Please click Retry to enter your temporary identification code again.

Need a new code?

You should receive your identification code shortly. If you haven't received it within a few minutes, please try again by clicking Get New Code

©2025 DFS Services LLC

2. The OTP could have expired. OTPs expire 5 minutes after they are generated. There will be a notice that appears on the OTP screen stating that "*The entered code is expired*" as illustrated in the below screen shot. If the code has expired, the User must request a new code by selecting "*Get New Code*".



For Added Security

Your temporary identification code has been sent to:

Email : Registered_Email_Address@TestingEmail.com

Once you receive your temporary identification code

Please enter it below:

The entered code is expired.

Your identification code for one-time use only.

Need a new code?

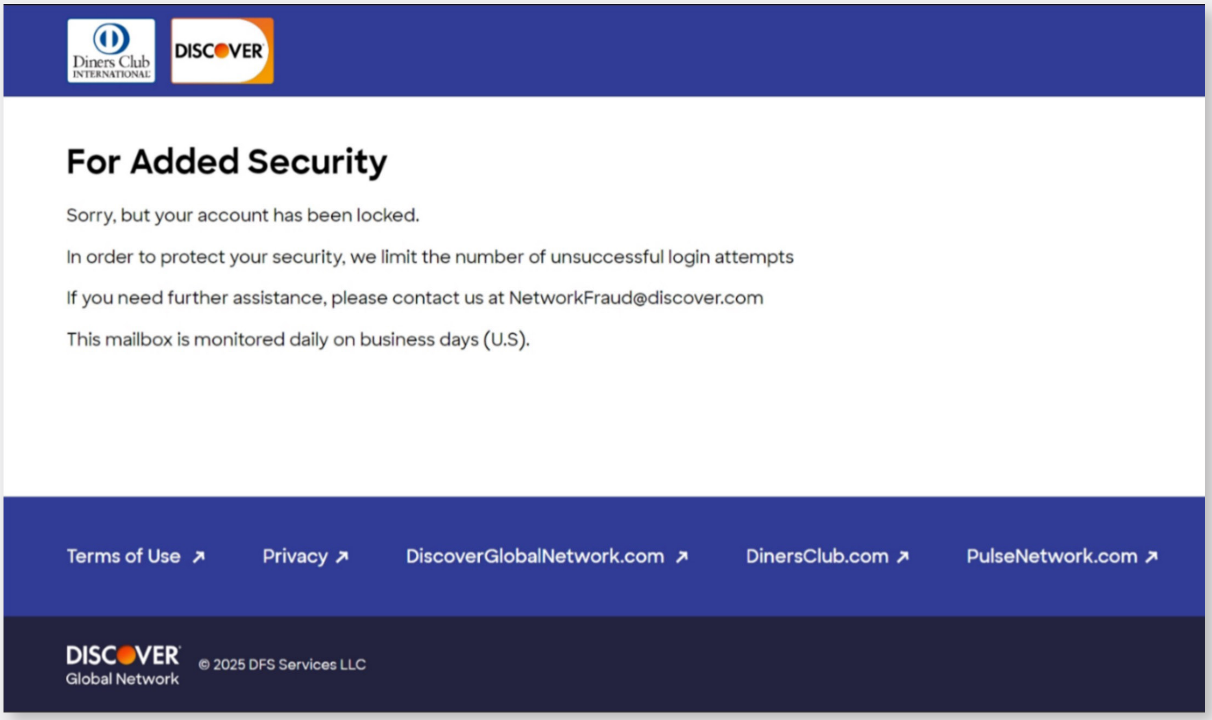
You should receive your identification code shortly.

If you haven't received it within a few minutes,

please try again by clicking Get New Code

©2025 DFS Services LLC

3. **The Users account could be locked. Please contact the support team at NetworkFraud@discover.com to unlock the account.**



For Added Security

Sorry, but your account has been locked.

In order to protect your security, we limit the number of unsuccessful login attempts

If you need further assistance, please contact us at NetworkFraud@discover.com

This mailbox is monitored daily on business days (U.S).

Publication Date: 3/6/2025

Internal and External Use Permitted

©2025 DFS Services LLC