Cantor Improved 2FA Setup Instructions

Step 1

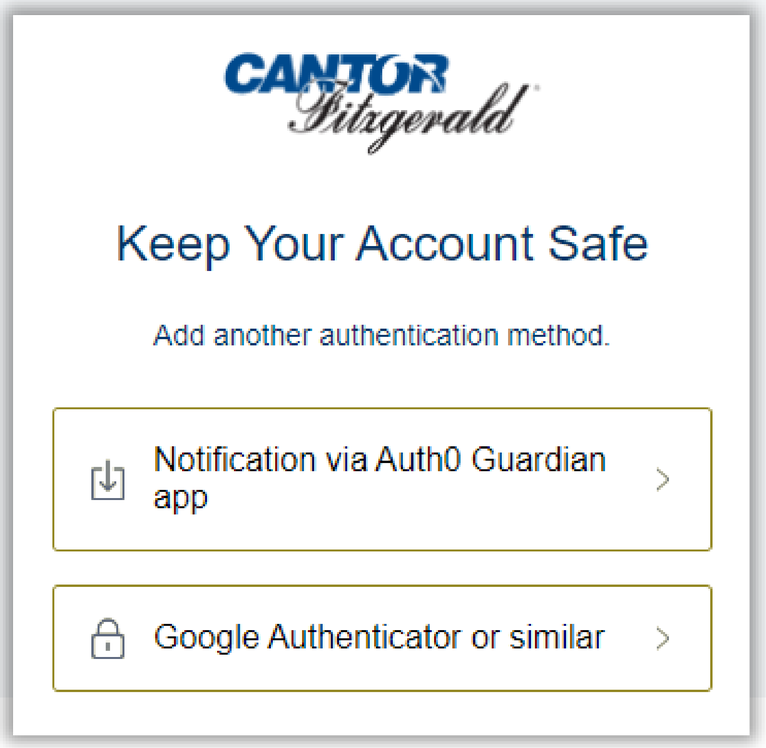
Setup 2FA

This process is to set up two-factor authentication (2FA) for your desktop login. You'll need a mobile phone to complete this setup and to sign in to your desktop in the future.

Previous users of 2FA on the client portal need to remove the existing 2FA before setting up the Cantor Improved 2FA.

1. **DESKTOP: Go** to; https://cantorportal.com/apex/r/mcext/cportal/

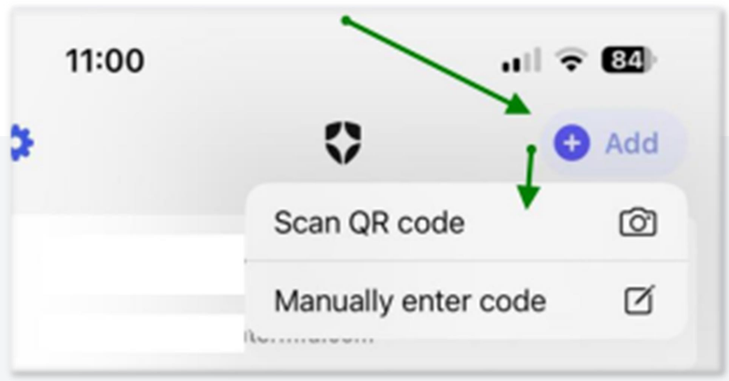
2. **DESKTOP**: Login to the portal using your Cantor credentials. Then click 'Notification via Auth Guardian app'



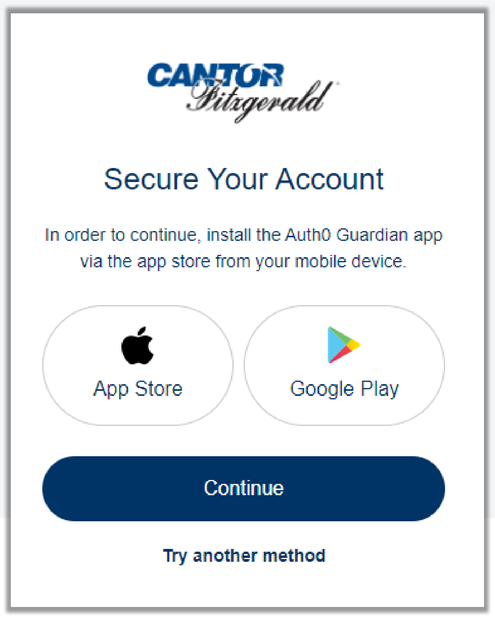
3. **MOBILE**: Now using your mobile - Go to your application store - App Store or Play Store.

4. **MOBILE**: Download the 'Auth0 Guardian' app.

5. **MOBILE**: Open the Guardian App and Click on Add 'Scan QR Code' and go back to your desktop computer for the nest step.

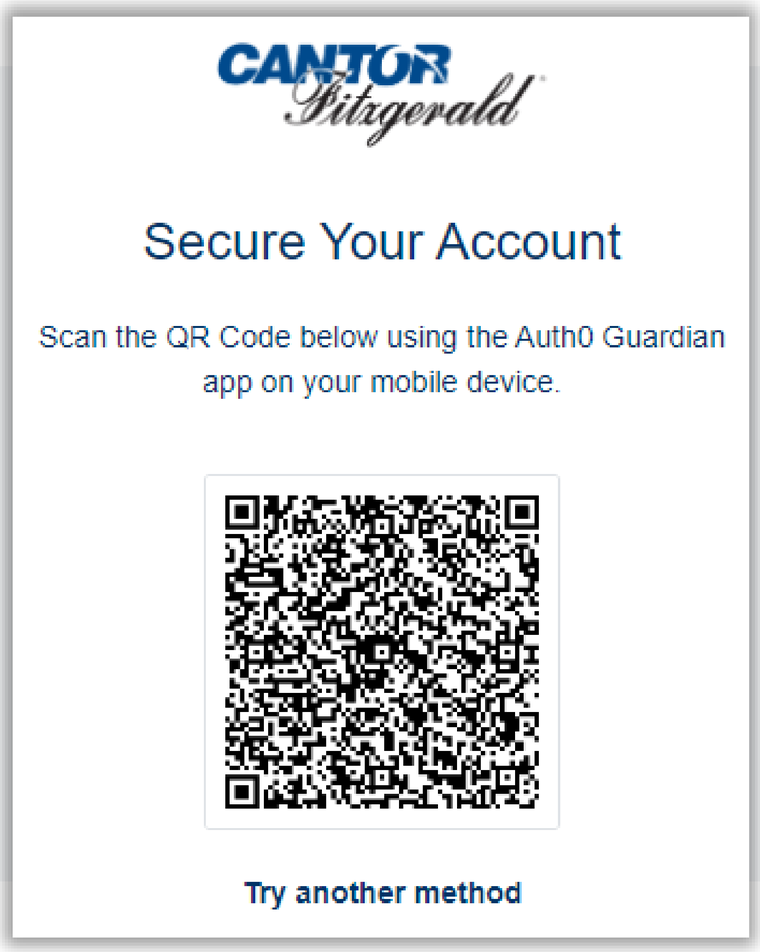


6. **DESKTOP**: Click 'Continue'.

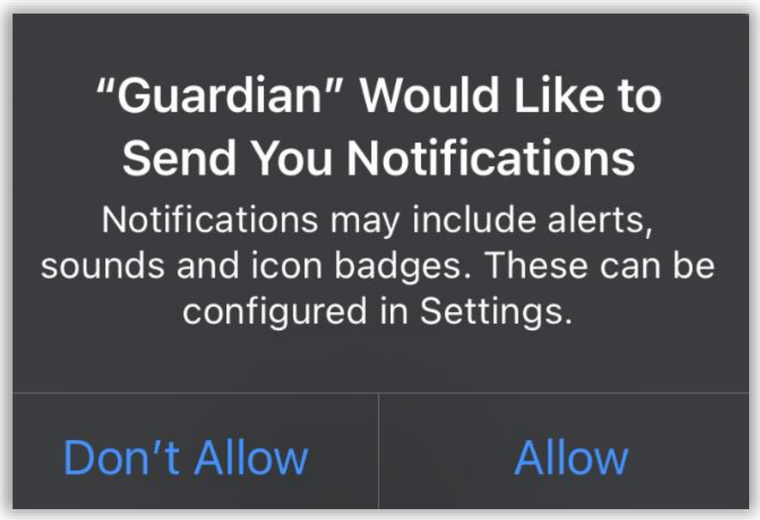


CANTOR Fitzgerald

7. **MOBILE**: On your mobile device, use the Auth0 Guardian app to scan the QR Code that's shown on your desktop screen.



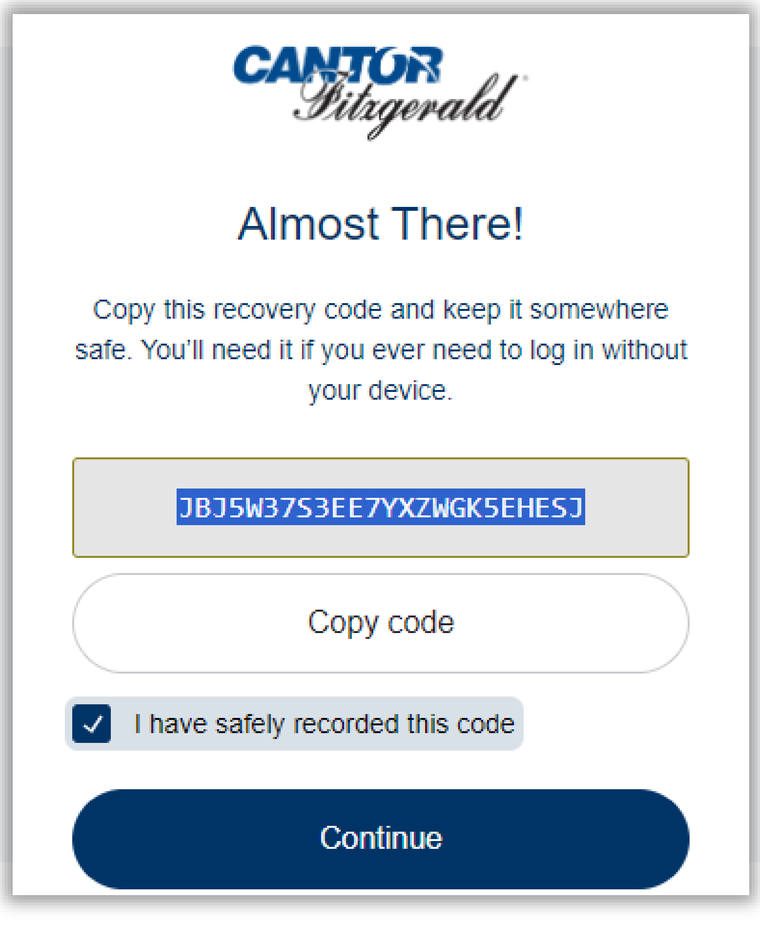
8. **MOBILE**: Tap "Allow" to permit the app to send you push notifications.



9. Take note of the Recovery Code on your Desktop Screen. You’ll need it if you ever need to log in without your device.

10. **DESKTOP:** Click on I have safely recorded this code’.

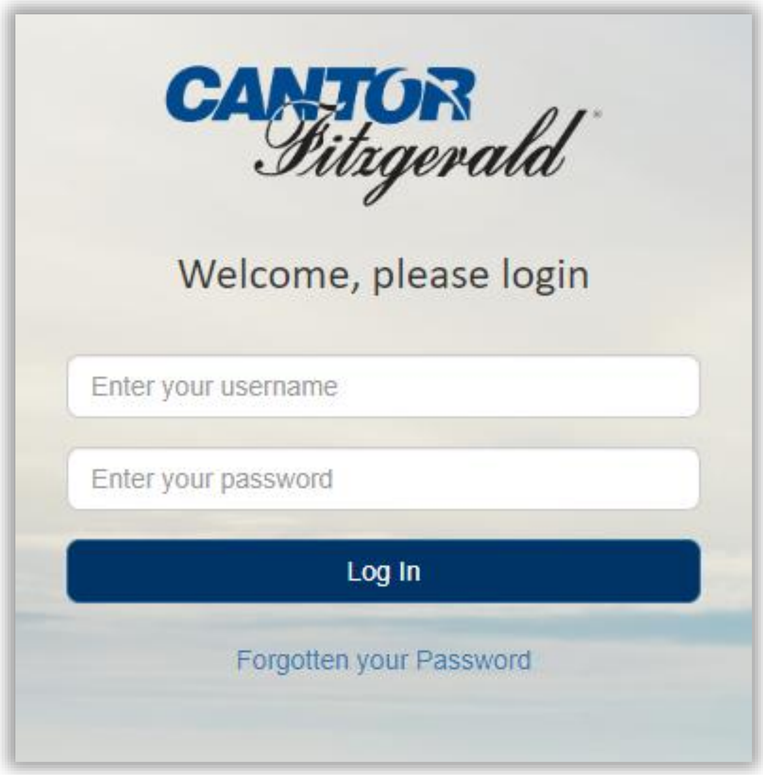
11. **DESKTOP:** Click ‘Continue’.



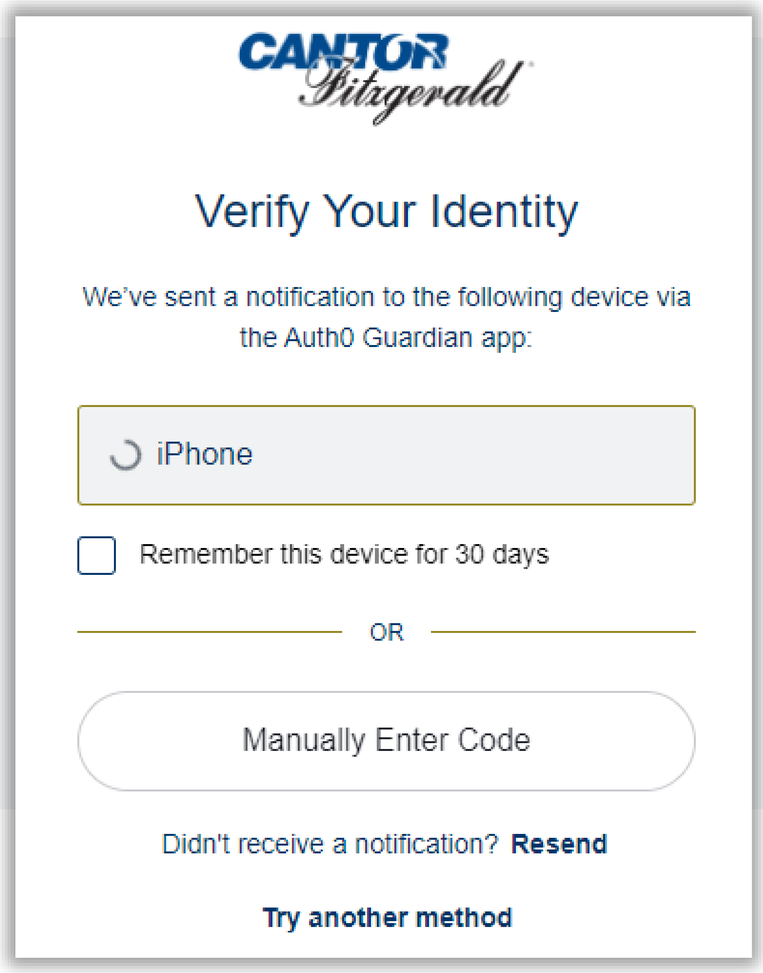
The two-factor authentication (2FA) setup is now successfully completed.

Step 2
Logging in with 2FA Setup.

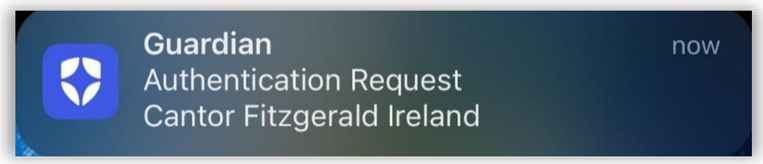
1. Log In with Cantor Portal Credentials.



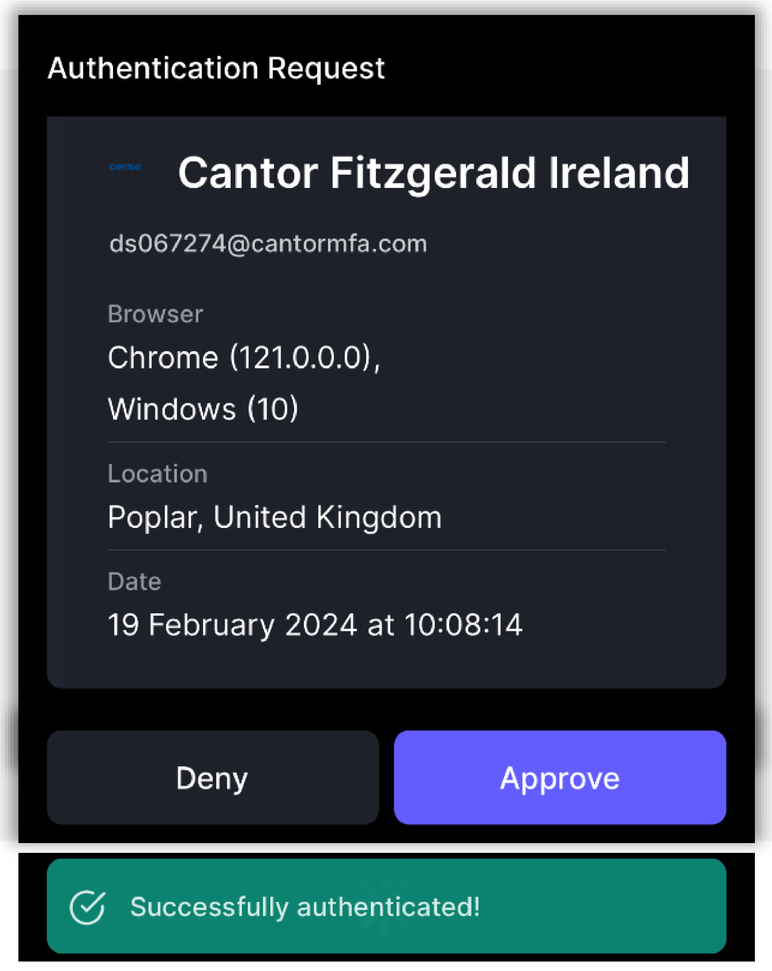
2. You will see this screen and a push notification will be sent to the device that you used to set up 2FA.



3. Click on the notification.



4. Click 'Approve'.



You have now logged in successfully using 2FA.

CANTOR Fitzgerald

Cantor Fitzgerald Insights
Personal Data Protection

At Cantor Fitzgerald Ireland, one of our core principles is protecting your personal data. This insight document will highlight to you the steps we are making to ensure best practices while also providing the highest level of security for the client portal through password protection and our newly improved two-factor authentication journey.

What is Two-factor Authentication?

2FA verifies your identity by using two independent factors: something you know like a password, something you are or have e.g., biometrics OR something you can get like a PIN code via a registered channel such as an application on your smart device or to your registered email.

Why are we making Two-factor Authentication mandatory?

This is to ensure your portal has the top level of security for your sensitive personal and financial information. It will mean that you and only you on authorised devices can access your client portal. By making 2FA mandatory, we are adding an extra barrier to entry that reduces the risk of unauthorised access, even if your password is compromised. The solution Cantor will provide to the client will be intuitive and allow for a smooth log on process while increasing the security of our portal for all parties.

Benefits of 2FA:

1. Increased Security: If someone hacks your password, they would still need the second factor, like your Face or Touch ID, to gain access to your account.
2. Peace of Mind: With 2FA, you can be confident that your personal information and financial data are safeguarded against potential threats. Knowing you have an extra layer of protection brings peace of mind.

Password Protecting Personal Devices: Strengthening Security Further

Why is password protection essential for personal devices?

Password protection on your smart device, be it a mobile phone or tablet, is crucial in preventing unauthorised access to your Cantor portal. In case of loss, theft, or leaving your device unattended, a strong password acts as the robust first barrier in preventing entry.

Simple Steps to Implement Password Protection:

1. Set a Strong and Unique Password: Create a password that combines uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable information such as birthdates, common words or consecutive numbers.
2. Enable Device Auto-Lock: Configure your device to automatically lock after a certain period of inactivity. This ensures your device is protected even if you forget to lock it manually.
3. Regularly Update Passwords: Change your device passwords periodically to maintain security. Consider using a password manager to securely store and generate strong passwords.

What happens in the event your device is stolen or lost?

- The perpetrator would still need the following to gain access to the clients Portal:
- Your portal password and your Face/Touch ID biometric to get into the portal.
- The device security lock PIN or password. This is a key reason in why we encourage you to practice the password protection steps noted above.