Protecting Your Identity

Identity theft is increasing as thieves and scammers seek to use your details to commit fraud. Accordingly, securing the privacy of your personal information is very important to us.

One way we can do this is with extra security when you log in to the secure online portal, something known as two-factor authentication (2FA). If you use internet banking then you are probably already familiar with how it works, with a code being sent to your mobile phone, which you then have to enter into the website or application you are using.

We don't have the resources of a bank, and we don't want to spend tens or hundreds of thousands of dollars of your money developing something. Instead, we recommend free third-party 2FA software offered by Google (called the Google Authenticator App). Note, you are welcome to use other authenticator apps, but we are unable to provide assistance with how to use it.

How To Set Up Google's Authenticator App

It's a relatively simple process to set up the 'Google Authenticator App', which works on both iOS (Apple) and Android mobile phone operating systems.

To assist, we have outlined what you need to do with step these -by-step instructions.

Step One

For iOS – visit Apple's App Store
For Android – visit the Play Store

And search 'Google Authentication App'. The software will have this logo:

!!!Warning!!! Be careful not to accidentally click on the paid advertisement of another authentication app. Make sure the app you download has the icon above.

If the app is already installed on your phone, skip to Step Three.

Step Two

Install the app on your phone. You may be required to input your phone's password.

Step Three

Once the Google Authentication App has been downloaded and installed, open the app by finding the icon (see above) in your available apps.

Step Four

Once the Google Authentication App is open, tap on the Get Started button.

This button will not appear if you have already installed the software. In this case, skip to Step Six.

Step Five

You will given the option to either:

1/ Log in with your Google account*; or

2/ Use the app without logging in

* If you do log in, Google Authenticator will save your 2FA data for you.

Make your choice to proceed.

Step Six

Click on the + button (shown below).

Step Seven

Click on 'Scan a QR code'

You may be asked for permission to allow the App to take pictures and record video. If so, click 'While using the app'.

If you prefer, you can also select 'Enter a setup key'.

Step Eight

It would be ideal if you could complete Steps Eight and Nine using your PC rather than on your phone.

Visit: https://portal.sogif.au/ and log in to your Strategic Opportunities (Growth & Income) Fund (SOGIF) account using your username and password.

Click the link 'Forgot your password' if you need to retrieve these details.

Step Nine

Once logged in, you will be automatically sent to the 'Two-Factor Authentication' screen as shown.
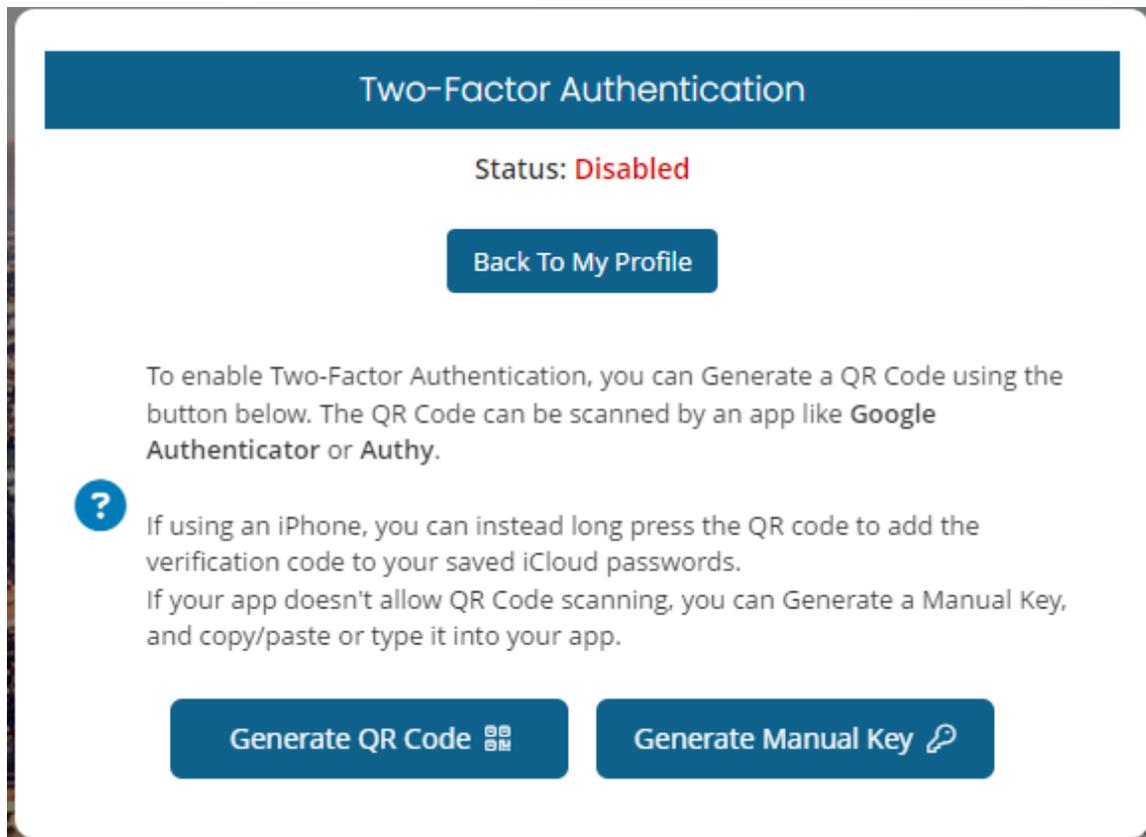
If you selected 'Scan a QR code' in Step Seven, click 'Generate QR Code' button.

Alternatively, if you chose 'Enter a setup key' in Step Seven, click the 'Generate Manual Key' button.
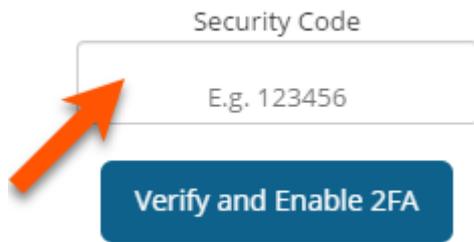
Step Ten

Return to the Google Authenticator App and either:

- use your camera to scan the QR code;
- type in the setup key.

Step Eleven

A verification code will appear in the app on your phone, under the heading 'Strategic Opportunities (Growth & Income) Fund.

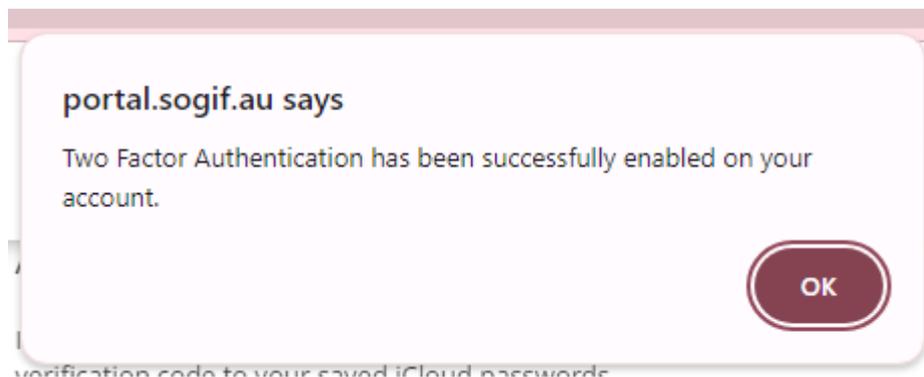Type this code into the area under the 'Security Code' in your SOGIF investor portal.

Step Twelve

Lastly, click the 'Verify and Enable 2FA' button.

Job Done!

Congratulations! You should have received this pop up notification confirming that 2FA has now enabled on your account.

Each time you log in to the secure investor portal will need to also input a code.

This code will be automatically generated in the Google Authenticator App, thereby securing your account from being accessed by anyone without the code.

To view the code, simply open the Google Authenticator App.

Need Help?

If you need further assistance, then please email admin@sogif.au