

## MULTIFACTOR AUTHENTICATION INSTRUCTIONS

To further protect your data and privacy, the Comer Family Foundation will enable multi-factor authentication (MFA) as a security precaution when logging into Foundant, our grants portal.

### What is multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is a security process that requires users to provide two or more different forms of identification to verify their identity when logging into an account or system. This adds an extra layer of protection beyond just a password, making it harder for hackers to gain access.

### How to Log On with MFA

To log in to Foundant, a user must provide authentication from two different sources:

1. This will be the password used to login to your Foundant account.
2. This will be an authenticator app downloaded onto your smartphone. Common apps for Apple and Android are Microsoft Authenticator, Google Authenticator, Authy, and 2FAS. Note: 2FAS has a browser extension that is recommended if you do not have access to a smartphone

**STEP ONE: Download an authenticator app to your smartphone. Options include but are not limited to:**

- [Microsoft Authenticator](#) - download from the Apple app store or Google Play store. The app will be named "Authenticator" once downloaded.
- [Google Authenticator](#) – download from the Apple app store or Google Play store. The app will be named "Authenticator" once downloaded.
- [Twilio Authy Authenticator](#) – download from the Apple app store or Google Play store. The app will be named "Authy" once downloaded.
- **If you do not have access to a smartphone, we recommend using a browser extension, such as [2FAS](#).**

### STEP TWO: Log on to Foundant with MFA

- Enter your email address and password in the Comer Family Foundation's grant site and click **Log On**.

Logon

Email Address\*

margaret.anderson@FTExample.org

Password\*

.....

Log On Create New Account

[Forgot your Password?](#)

- Enter the provided key into your two factor application, or scan the QR code provided.
- Open the Authenticator app on your phone. Your multi-factor application will provide you with a token. Enter the token into the Foundant GLM/SLM Verification Code field, and then click **Verify**. (See sample image below.)
- The next time you log on to the GLM/SLM site, your email address, password, and authentication code will be required.

Two-Factor Authentication

To enable two-factor authentication, follow these steps:

1. Download a two-factor authenticator app like Authy or Google Authenticator.
2. Enter this key in your app: `QC2S 4TYS NNVD FOBR KYAY T5RA QC5G IL4M` 

or, scan the following QR code with your app:



3. Once you have scanned the QR code or input the key above, your two-factor authentication app will provide you with a unique code. Enter the code in the confirmation box below.

Verification Code

