Multi-Factor Authentication (MFA)

— When will MFA be required?

Beginning November 13, 2023 FACTS will roll out MFA for consumer users (families) that access the following FACTS products:

- FACTS Tuition Management
- FACTS Grant & Aid Assessment

FACTS SIS will begin requiring MFA in early 2024.

Note: FACTS SIS is the Family Portal (formerly RenWeb).

— Why is FACTS requiring this change?

The security of your school and family data is at the forefront of each and every decision we make at FACTS. As more aspects of our lives become dependent upon our ability to access information through mobile and cloud-based services, it has become increasingly important to ensure the integrity of the users behind the devices attempting to access this information.

In support of our commitment to providing the highest levels of security for our products, FACTS has made the decision to begin utilizing multi-factor authentication (MFA).

Choose an authenticator app

An authenticator app is an app that adds MFA to accounts that you want to protect. When you set up your account for MFA, you will receive a secret key to enter into the authenticator app. This establishes a secure connection between the authenticator app and your account.

Authenticator apps can be installed on your smartphone and/or desktop computer. Apps such as Authy offer both a phone and desktop version. You can add an account to an existing authenticator app, or, if you do not already have an authenticator app, some of the most common ones are:

- Google Authenticator
- Microsoft Authenticator
- Authy by Twilio (includes desktop version)
- LastPass
- 2FA Authenticator
- Duo Mobile
- Aegis Authenticator

Set up multi-factor authentication

You can sign up for multi-factor authentication using an authenticator app or an email, depending on your preference. We recommend setting up using an authenticator app for increased security because apps don't send messages, like SMS or email, that someone could intercept.

Instructions for how to set up MFA are provided below.

— Sign up using email

1. Click **Begin**.
2. Click **Sign Up Using Email**.
   - If only one email is stored on your profile, the authentication code will automatically be sent to that email address.
   - If you have multiple email addresses saved to your profile, select the one where you'd like the authentication code sent.
3. Click **Send Code to Email**.
4. Check your email inbox to access your one-time use code. (See below.)
5. Type the provided code in the Authentication Code text box.
6. Click **Submit**.
7. Choose two authentication questions and provide answers.
8. When finished, click **Save** to log in to your account.

> 💡 **Tip**
> If you cannot find your emailed authentication code, check your junk mail folder or click **Resend Code to Email** to generate a new email.

Example (see below)

Verify your identity

University

Hello Amanda,

Here is your one-time code to complete signing in.

557298

For security purposes, this code will expire in 10 minutes.

If you didn't make this request, please secure your account.

Thank you,
Nelnet Campus Commerce

— Sign up using an app

> ⚠️ **Important**
> If you choose to enroll using an authenticator app, but don't yet have an established app, download one before proceeding.

1. Click **Begin**.
2. Click **Sign Up Using App**.
3. To register:
   - Using an authenticator app on your smartphone, scan the QR code or type in the code provided.
   - Using an authenticator app on your desktop, copy and paste the code provided.
4. Follow the remaining setup prompts in your authenticator app.
5. Once completed, return to the MFA setup screen and click **Next**.
6. Enter a **Verification Code** from your app to ensure that the app is appropriately linked to your account.
7. Click **Next**.
8. Select **Print** or **Download**. In the event that you lose your device or cannot access your authenticator app, these backup recovery codes can be used to access your account and should be stored in a safe place.
9. Click **Next**. Multi-factor authentication is complete.
10. Click **Next** to choose authentication questions and answers.
11. Choose two authentication questions and provide answers.
12. When finished, click **Save** to log in to your account.

> 📋 **Can I change my authentication method after setting it up?**
> Yes! You may change your preferred authentication method by contacting your FACTS account management team to request a reset of your MFA configuration.

— How often will I be prompted to authenticate?

The authentication token remains active for 4 hours. If it has been more than 4 hours since the last authentication and the user signs out, they will be prompted to reauthenticate when signing in.

Log in with multi-factor authentication

After you have completed MFA setup, you will be prompted to authenticate for each login. Learn how to log in with MFA for each method below.

Expand/Collapse All

— Using email

1. Select your preferred email address and click **Send Code to Email** if you have multiple email addresses saved in your profile. If you have only one email stored on your profile, the authentication code will automatically be sent to that email address.
2. Check your email inbox to access your one-time use code.
3. Type the provided code in the Authentication Code text box.
4. Click **Submit** to log in to your account.

— Using an authenticator app

1. Open your authenticator app to receive the verification code.
2. Type the provided code in the Verification Code text box.
3. Click **Verify** to log in to your account.

— Using a backup recovery code

If the device you authenticate with has been lost, stolen, or damaged, you can use a backup recovery code to authenticate into your account.

If you did not save the recovery codes when you signed up for MFA or lost the codes, you can contact FACTS customer service to have your MFA reset. You will be prompted to set up authentication again the next time you log into FACTS.

1. If you do not have access to your device or authenticator app, click **Don't have access to app.**
2. Type a backup recovery code from your previously downloaded or printed list into the Recovery Code text box. (See *Sign Up Using App* above.)
3. Click **Submit** to log in to your account.

> **Note**
> After the use of a backup recovery code, you will receive an email notifying you of its use. Each code is valid for one-time use only.