Frequently Asked Questions:
Two Factor Authentication and Aggregator Access

What is Two Factor Authentication?
Two-factor authentication (2FA) adds a second level of authentication security to your online 529 account. Entering only your username and one password is considered a single-factor authentication. 2FA requires you to have two out of three types of credentials before being granted access to your account. The three types of credentials are:

- Something you know, such as a verification code, personal identification number (PIN), or password;
- Something you have, such as an ATM card, phone or secure token; and
- Something you are, biometrics such as fingerprint, voice print or retinal scan

Why is Two Factor Authentication important?
Security of your confidential information is a top priority. In this age of phishing attacks and identity thefts, relying on username and password alone do not guarantee security. No matter how strong or complex your primary password might be, your account stands the risk of a security breach if your password falls into the wrong hands.

Is Two Factor Authentication a new security authentication mechanism?
No. For instance, using your ATM card is a form of 2FA. You must provide the physical card (something you have) along with your PIN (something you know) in order perform a financial transaction.

Is Two Factor Authentication difficult?
No. 2FA might seem like an inconvenience, but if you are willing to wait a few extra seconds, you will be rewarded with a higher level of security of your online 529 account.

How does Two Factor work?
When you sign into your account, as you normally would with a username and password, you will be prompted to select how you want your PIN delivered (i.e., an automated call or a text message). You'll then receive the PIN via your selected method of delivery and you will be asked to enter this PIN into the designated box and follow the remaining instructions.

What is a PIN?
A PIN is a one-time personal verification code that is delivered via a text message, an automated call or by a customer service representative over the phone.

How are Two Factor Authentication PINs delivered?
You will be able to select any of the following options; **SMS text** to a mobile number, **Robo call** to a phone number or you may **call into our call center** and speak with a customer service representative.

Will I need to enter a PIN every time I log in to my 529 online account?
It depends. Once you authenticate your device and designate it as a trusted device, you will not be required to enter a PIN the next time you login from that same device. You will only need to provide your username and password. If you are logging in from a new device, you will be prompted to enter a PIN again, since that device is not recognized as a trusted device. Note that if you have not logged-in from a trusted device for longer than 6 months, you will be asked to authenticate that device again.

What is a trusted device?
A trusted device is a private device that you routinely use, and one that strangers do not have access to.

What if I forgot my password?
If you've forgotten your password, simply follow the prompts under option for "Forgot my Password".

What if I don't have access to my trusted device?
If you don't have access to your trusted device you may connect from another device but will be prompted to enter a PIN.

What if didn't receive my PIN?
If you didn't receive a PIN then you may request the system to generate another. PINs are only valid for 5 minutes from the time they are generated. Once you've requested a new PIN the previous one becomes invalid.

If I can't sign in, how do I regain access to my account?
Call customer service and they will be able to assist you.

What are Aggregators?
Aggregators provide a service that allows users to combine their balance and activity information from various financial accounts into a single view (e.g., a dashboard).

How do aggregators work?
Aggregators use a form of technology called data scraping. Data scraping is the process of extracting information from designated web sites. In this instance, the aggregator will login to your account using your personal security credentials to extract information from your account.

How do Aggregators access 529 online account balance and activity information?
In order for an aggregator to gain access to a 529 online account, the account owner has to provide that aggregator with his or her existing username and password in order for that aggregator to "scrape" data from his or her account screens.

How does Two Factor Authentication affect Aggregators accessing my 529 online account?
Essentially, use of 2FA will break aggregator access. This will happen because aggregators will not be able to use your existing login credentials to access your account once you authenticate your device with a PIN. For that reason, should you desire to continue to provide access to your aggregator, sign into your account and create an aggregator read only account, prior to enabling 2FA.

What is an aggregator read only account and does this benefit me?
The read only aggregator account, once created, will allow the aggregator to access only non-sensitive information within your account via a different username and password.

This benefits your security because the read only aggregator account will allow the aggregator to access only the information needed to create your financial view, which are basic account and investment details along with account transactions. The aggregator will no longer have access to your sensitive personal information.