TWO-FACTOR AUTHENTICATION GUIDE

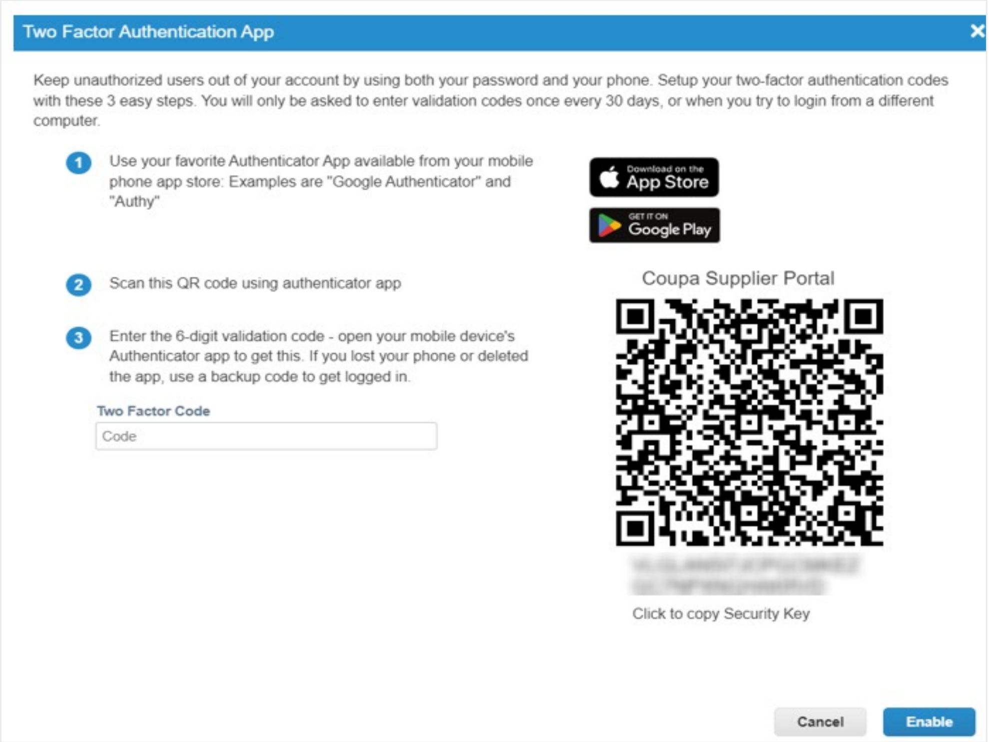
Two-factor authentication (2FA) is optional for the suppliers to set up on their CSP account.

A Two-Factor Authentication prompt may be presented to every Supplier when first logging into the Coupa Supplier Portal, and to existing suppliers who haven't yet set-up this function.

It is an optional feature that can be closed by clicking the 'x' or 'Cancel' button.

THE 2FA SCREEN PRESENTED:

- When logging-in, suppliers (existing or new supplier) may be prompted with the screen below.



Two Factor Authentication App

Keep unauthorized users out of your account by using both your password and your phone. Setup your two-factor authentication codes with these 3 easy steps. You will only be asked to enter validation codes once every 30 days, or when you try to login from a different computer.

1. Use your favorite Authenticator App available from your mobile phone app store: Examples are "Google Authenticator" and "Authy"
2. Scan this QR code using authenticator app
3. Enter the 6-digit validation code - open your mobile device's Authenticator app to get this. If you lost your phone or deleted the app, use a backup code to get logged in.

Two Factor Code

Code

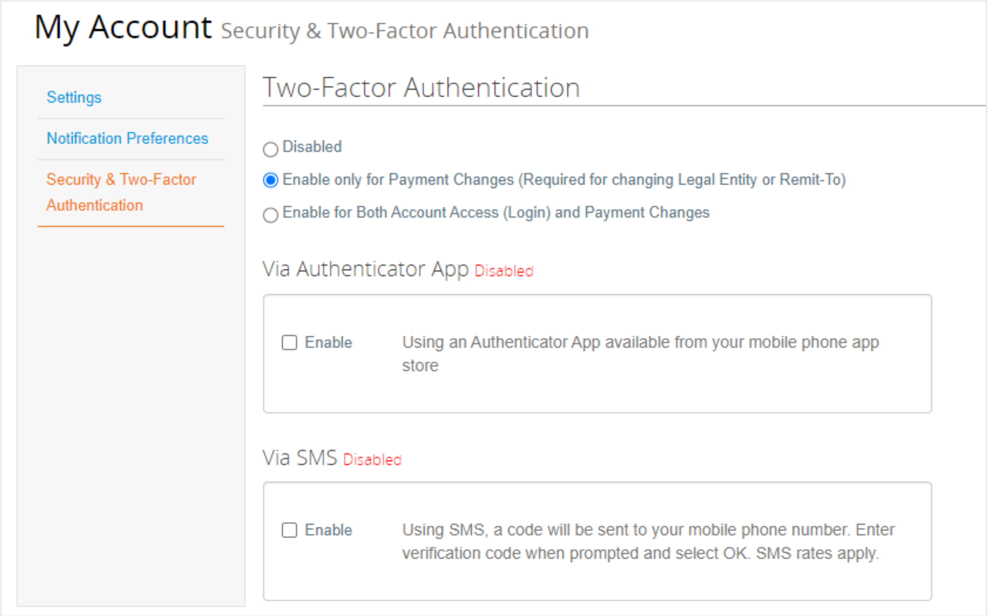
The supplier has the following options to choose:

1. **Option 1** Click "**Cancel**" then navigate out of the Two Factor Authentication setting screen.
2. **Option 2** Click "**Cancel**" and choose to "**Disable**" 2FA then save.
3. **Option 3** Click on the "**Enable**" button to set up the 2FA (optional)

See below for more information on each option.

Option 1: If you decide not to set up Two Factor Authentication now and prefer to set up at a later date, click "**Cancel**" to exit the pop-up window.

Note the below screen is displayed and default 2FA is "**Enable only for Payment Changes (Required for changing Legal Entity or Remit-To**)". This won't trigger 2FA as the notification preferences (via App Authenticator App or via SMS) to receive authentication codes are still disabled.



My Account Security & Two-Factor Authentication

Two-Factor Authentication

○ Disabled

● Enable only for Payment Changes (Required for changing Legal Entity or Remit-To)

○ Enable for Both Account Access (Login) and Payment Changes

Via Authenticator App Disabled

□ Enable — Using an Authenticator App available from your mobile phone app store

Via SMS Disabled

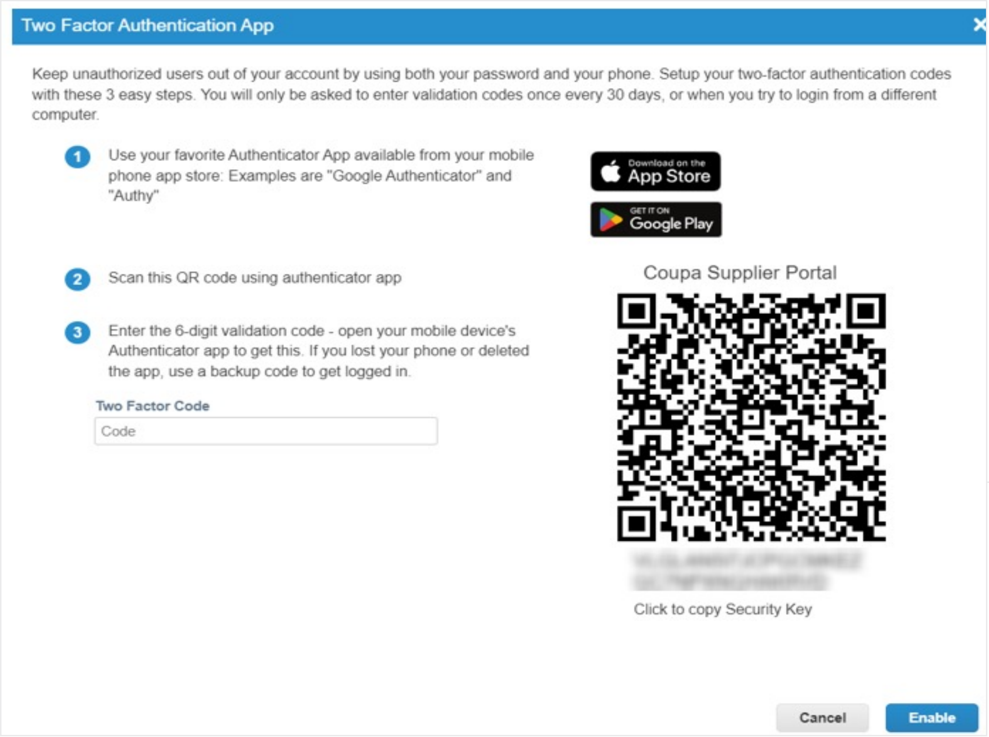
□ Enable — Using SMS, a code will be sent to your mobile phone number. Enter verification code when prompted and select OK. SMS rates apply.

Option 2: Click "**Cancel**" to exit the pop-up window and choose "**Disabled**" if decided not to proceed with set up of Two Factor Authentication.

Please note that you can still re-enable it anytime if needed by going to ***My Account > Account Settings > Security & Two-Factor Authentication***

Option 3: To Enable 2FA. **Once 2FA is enabled, you can no longer disable it.**

If you want to Enable 2FA, follow the steps provided on the screen. Once the Authentication App is installed on your phone, enter the OTP code generated on the App and paste it on the "Two Factor Code" field then click "**Enable**".



Two Factor Authentication App

Keep unauthorized users out of your account by using both your password and your phone. Setup your two-factor authentication codes with these 3 easy steps. You will only be asked to enter validation codes once every 30 days, or when you try to login from a different computer.

1. Use your favorite Authenticator App available from your mobile phone app store: Examples are "Google Authenticator" and "Authy"
2. Scan this QR code using authenticator app
3. Enter the 6-digit validation code - open your mobile device's Authenticator app to get this. If you lost your phone or deleted the app, use a backup code to get logged in.

Two Factor Code: Code

Coupa Supplier Portal

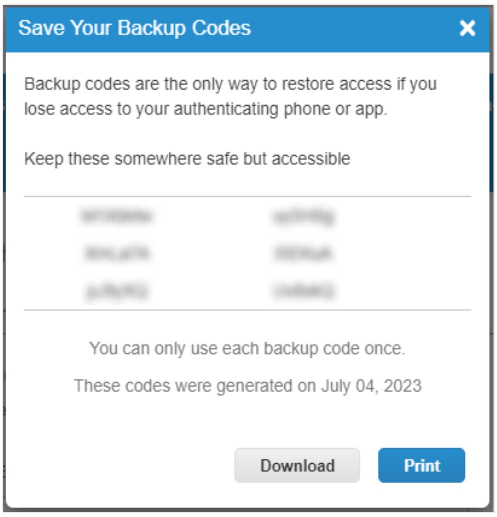
[redacted]

Click to copy Security Key

A list of Backup Codes will pop-up which can be used to restore access in case you lose access to your authenticating phone or app.

NOTE:

You can only use a recovery code once, so refresh your list if you have to use a recovery code. Go to **Account Settings > Security & Two-Factor Authentication** and click Regenerate Recovery Codes to get a new list of codes.



Save Your Backup Codes

Backup codes are the only way to restore access if you lose access to your authenticating phone or app.

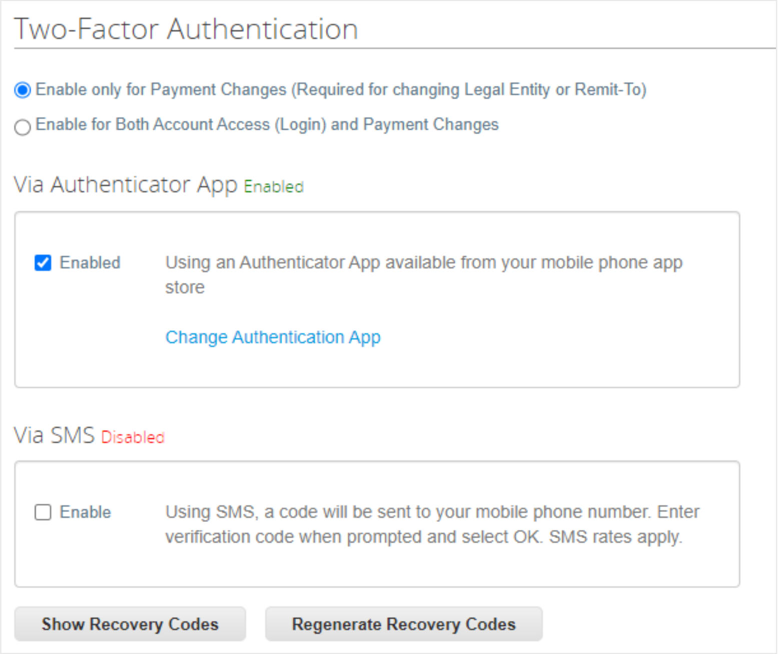
Keep these somewhere safe but accessible

[redacted]

You can only use each backup code once.

These codes were generated on July 04, 2023

Once done, this will automatically enable the 2FA via Authenticator App



Two-Factor Authentication

● Enable only for Payment Changes (Required for changing Legal Entity or Remit-To)
○ Enable for Both Account Access (Login) and Payment Changes

Via Authenticator App Enabled

☑ Enabled — Using an Authenticator App available from your mobile phone app store

Change Authentication App

Via SMS Disabled

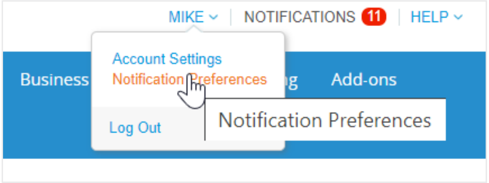
□ Enable — Using SMS, a code will be sent to your mobile phone number. Enter verification code when prompted and select OK. SMS rates apply.

When you enable two-factor authentication, you can choose from the two following options:

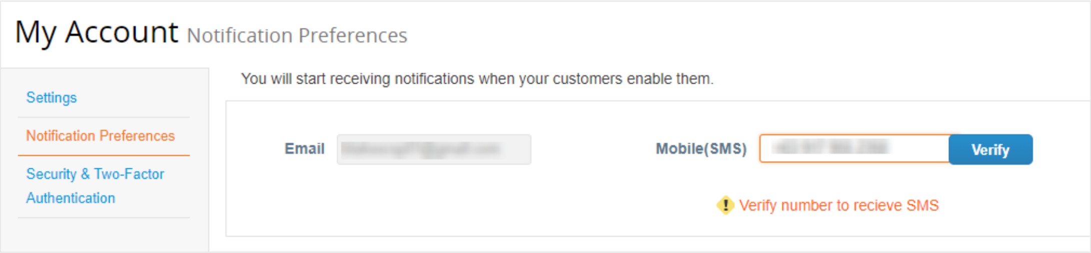
- **For Payment Changes (Required for Changing Legal Entity or Remit-To):** Two-factor authentication is required when creating or editing legal entities, remit-to, and bank account information.
- **For Both Account Access (Login) and Payment Changes**: Two-factor authentication is required when logging in to the CSP. You don't have to reauthenticate when working with financial data because you already authenticated when logging in.

Depending on how you want to receive the verification codes, select one of the following options and set your preference as the default:

- **Via Authenticator App** to use an authenticator app available from the app store on your mobile phone. Two-factor authentication (2FA) through an authenticator app is the preferred method. (Refer to the instructions above)
- **Via Text Message** to use a code sent by text message to your phone number. If you want to receive text message (SMS) notifications or verification codes, you must enter and validate your phone number under **My Account > Notification Preferences.**



Enter Mobile (SMS) then click **Verify.**



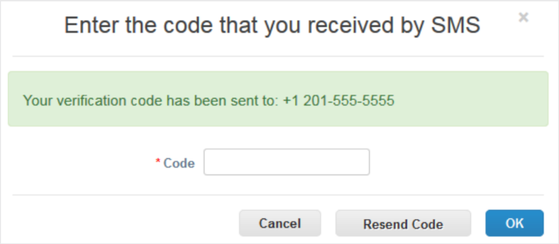
My Account Notification Preferences

You will start receiving notifications when your customers enable them.

Email [redacted] Mobile(SMS) [redacted]

! Verify number to recieve SMS

Enter the verification code in the pop-up window sent to your mobile and click OK.

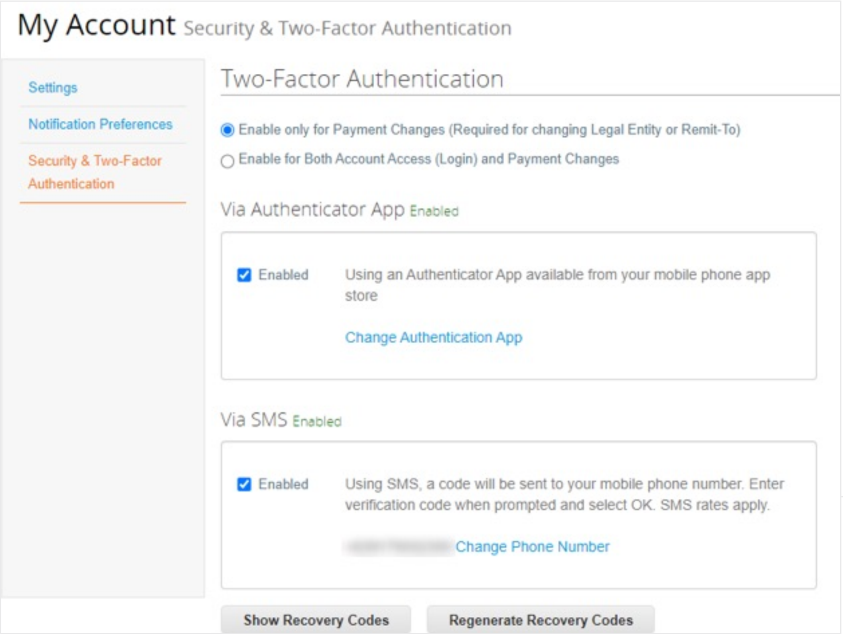


Enter the code that you received by SMS ×

Your verification code has been sent to: +1 201-555-5555

* Code

2FA is now enabled via Authenticator App and SMS successfully.



My Account Security & Two-Factor Authentication

Two-Factor Authentication

● Enable only for Payment Changes (Required for changing Legal Entity or Remit-To)

○ Enable for Both Account Access (Login) and Payment Changes

Via Authenticator App Enabled

☑ Enabled Using an Authenticator App available from your mobile phone app store

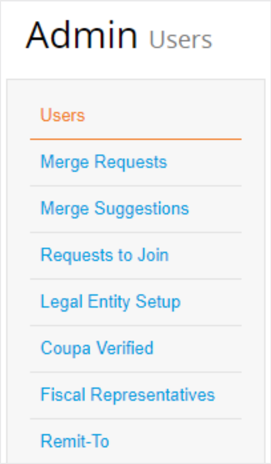
Change Authentication App

Via SMS Enabled

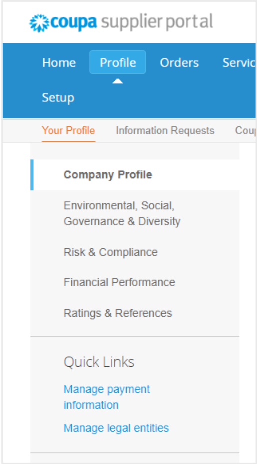
☑ Enabled Using SMS, a code will be sent to your mobile phone number. Enter verification code when prompted and select OK. SMS rates apply.

[redacted] Change Phone Number

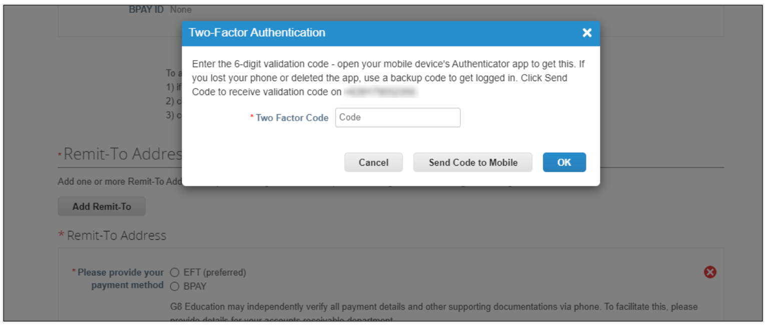
Once 2FA is completed, suppliers now may see Two-Factor Authentication on **Legal Entity and Remit-To pages** in the CSP. **Go to Setup > Remit To or Setup > Legal Entity Setup** or **Profile Tab > Quick Links.**



Admin Users



2FA is also now prompted when adding/updating Bank Information and Remit-To Address during the SIM form completion.



BPAY ID None

Two-Factor Authentication ✕

Enter the 6-digit validation code - open your mobile device's Authenticator app to get this. If you lost your phone or deleted the app, use a backup code to get logged in. Click Send Code to receive validation code on [redacted]

* Two Factor Code: Code

Cancel | Send Code to Mobile | OK

* Remit-To Addres

Add one or more Remit-To Add

Add Remit-To

* Remit-To Address

* Please provide your payment method: ○ EFT (preferred) ○ BPAY

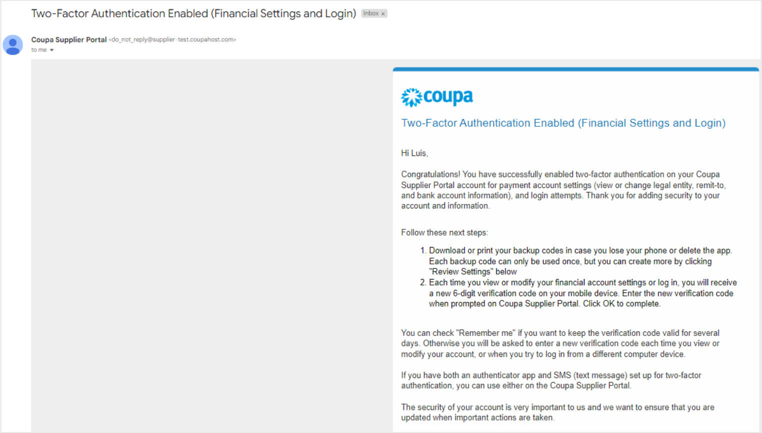
G8 Education may independently verify all payment details and other supporting documentations via phone. To facilitate this, please provide details for your accounts receivable department

NOTE:

The code is only good for 60 seconds. If you do not type that code on the CSP sign-in page and click Log In within 60 seconds, you must get a new code and try again.

When you enable two-factor authentication, you get an email notification of the change.

- Enable only for Payment Changes (Required for changing Legal Entity or Remit-To)



Two-Factor Authentication Enabled (Financial Settings and Login) Inbox ×

Coupa Supplier Portal <do_not_reply@supplier-test.coupahost.com>
to me

coupa

Two-Factor Authentication Enabled (Financial Settings and Login)

Hi Luis,

Congratulations! You have successfully enabled two-factor authentication on your Coupa Supplier Portal account for payment account settings (view or change legal entity, remit-to, and bank account information), and login attempts. Thank you for adding security to your account and information.

Follow these next steps:

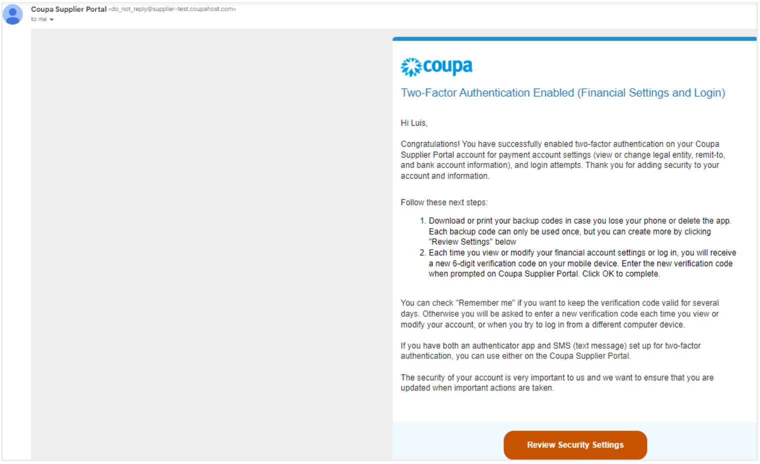
1. Download or print your backup codes in case you lose your phone or delete the app. Each backup code can only be used once, but you can create more by clicking "Review Settings" below
2. Each time you view or modify your financial account settings or log in, you will receive a new 6-digit verification code on your mobile device. Enter the new verification code when prompted on Coupa Supplier Portal. Click OK to complete.

You can check "Remember me" if you want to keep the verification code valid for several days. Otherwise you will be asked to enter a new verification code each time you view or modify your account, or when you try to log in from a different computer device.

If you have both an authenticator app and SMS (text message) set up for two-factor authentication, you can use either on the Coupa Supplier Portal.

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

- Enable for Both Account Access (Login) and Payment Changes



Coupa Supplier Portal <do_not_reply@supplier-test.coupahost.com>
to me

coupa

Two-Factor Authentication Enabled (Financial Settings and Login)

Hi Luis,

Congratulations! You have successfully enabled two-factor authentication on your Coupa Supplier Portal account for payment account settings (view or change legal entity, remit-to, and bank account information), and login attempts. Thank you for adding security to your account and information.

Follow these next steps:

1. Download or print your backup codes in case you lose your phone or delete the app. Each backup code can only be used once, but you can create more by clicking "Review Settings" below
2. Each time you view or modify your financial account settings or log in, you will receive a new 6-digit verification code on your mobile device. Enter the new verification code when prompted on Coupa Supplier Portal. Click OK to complete.

You can check "Remember me" if you want to keep the verification code valid for several days. Otherwise you will be asked to enter a new verification code each time you view or modify your account, or when you try to log in from a different computer device.

If you have both an authenticator app and SMS (text message) set up for two-factor authentication, you can use either on the Coupa Supplier Portal.

The security of your account is very important to us and we want to ensure that you are updated when important actions are taken.

WHERE DO I GO IF I NEED HELP?

- For all procurement-related enquiries, email **themarketplacesuppliers@g8education.edu.au**
- For technical assistance with Coupa go to: **supplier.coupa.com/help/** - if you cannot find an answer there, use the online **Chat with Coupa Support**