# Originator/User CAFT Multifactor Authentication FAQs

## 1. What has changed with respect to logging into CAFT?

PPJV has introduced multifactor authentication (MFA) to the CAFT platform to further increase cybersecurity and deter fraudulent access.

Previously, users would log in directly to CAFT by entering their user ID and password into the CAFT home page. Now, users arriving at the CAFT site (caft.paymentsanytime.com) will be first redirected to an MFA login process, where they will need to input a time-based, one-time password (TOTP) generated via an authenticator app. Once MFA verification is complete, users will reach the CAFT login screen to which they are accustomed, where they will enter their user ID and password credentials as before.

## 2. What is multifactor authentication and why is it important to use?

Multifactor authentication (MFA) adds a layer of security to online accounts. It requires users verify their identity through two or more authentication process. For example, the CAFT MFA process requires users to input a time-based, one-time password (TOTP) generated by an authentication app, such as Microsoft or Google Authenticator, installed on their device.

MFA deters illegitimate access to an account. While a fraudster might be able to obtain an account holder's login credentials through a remote data breach or phishing attack, it is significantly harder for the fraudster to also gain access to a user's device where the TOTP authentication code is generated.

MFA applications like that now being used for CAFT are sometimes also called two-step verification or 2FA because there are two factors required for verification (password and one-time code).

## 3. How do I enable MFA? What's an authentication app and how do I get one?

To enable MFA, your first step will be to download an authentication app to your smartphone or tablet.

An authentication app is an app designed to provide special time-based one-time passwords whenever you log into a registered application. These temporary codes or passwords help ensure a fraudster can't gain access to your accounts even if your password is compromised.

The CAFT MFA is configured to work with several different authentication apps. We recommend using either Microsoft Authenticator or Google Authenticator. Both apps are free, secure and easily downloadable from the Apple and Google app stores. (Note, you may have previously installed one of these authentication apps to access a different account, such as for work or banking. If so, the app can also be used for CAFT MFA).

Once you've installed an authenticator app to your device, you'll be able to register for CAFT MFA. The first time you access CAFT after December 6, you'll be shown a QR code. Start your authentication app and scan the QR code: this will register your CAFT MFA account with the app. From this point forward, you can check the authenticator app for the code you'll need each time you log into CAFT. *(Refer to the CAFT MFA User Guide sent to you along with these FAQs for a detailed walkthrough of this process, including screenshots).*

## 4. I'm having issues setting up MFA, who can I contact for support?

Please contact your usual CAFT support contacts at Access Credit Union.

## 5. Why can't I scan in the QR code using the authenticator app?

There may be a number of reasons for a QR code not scanning in properly such as the camera being slightly out of focus or too far away. If this happens, try again, making the QR code larger if possible (though still within the designated square) and holding the camera steady for a few seconds.

If the QR code simply won't work, there is an alternative method. You can click the green 'Trouble Scanning?" link under the QR code. An alphanumeric code will appear which you can type into the authenticator app in lieu of scanning the QR code.

## 6. Why did my one-time code not work?

The authenticator app generates a new one-time code every 30 seconds. Make sure you give yourself enough time to enter the code before it resets (i.e., if there are only a few seconds left on a timer, wait for a fresh code and input that). Also, if you have multiple accounts on your Authenticator app, make sure to select the code under the CAFT account.

If you see the error message "Too many failed codes. Wait for minutes before retrying" it means you've tried too many times with the wrong or expired code. You will need to wait about 15 minutes before trying again.

## 7. What happens if I get locked out of my account?

Your MFA account will become locked after too many failed login attempts. If this happens, please contact your usual CAFT support contacts at Access Credit Union and they can assist unlocking your account.

## 8. What is a recovery code? Why do I need one?

When you register your CAFT account in your authenticator app, you will be given a one-time-use recovery code. This code can be used exactly once to log in when you don't have access to your authenticator app. (For example, you've misplaced your smartphone or it has run out of power).

Remember to make a copy of this recovery code when you register for MFA and store it somewhere safe (preferably separate from your login credentials). Note: when a one-time recovery code is used, a new recovery code will be generated by the MFA system which you can again copy and keep safe in case of future need.

## 9. What if I lose my recovery code?

If you lose your recovery code and need to log in without the device on which you installed the authenticator app, please contact your usual CAFT support contacts at Access Credit Union.
and they will assist you.

## 10. I tried to log in but got an error message telling me my account is disabled. What do I do?

You will need to have your account reset. Please contact your usual CAFT support contacts at Access Credit Contact and they can assist you.

## 11. What username and password do I enter on the CAFT MFA login screen?

You should enter your usual CAFT username password combination—the same one you would have used prior to the implementation of MFA. Note: you will need to enter your username/password credentials twice: once at the beginning of the new MFA process, and again when you arrive at the main CAFT login screen.

## 12. What do I do if I've forgotten my CAFT password or my password has expired?

If your password has expired, you will still be able to enrol in MFA and will have the opportunity to update your password once you reach the CAFT login page.

However, if you've forgotten your password, you will not be able to reset the password on your own. You will need to request a password reset through your regular CAFT support contacts.

## 13. Do I have to enter an authentication code every time I log in?

You will need to enter your one-time MFA code almost every time you login to CAFT. The one exception is if you logout and log back in during a single session—i.e., you log in on the same browser and device within 8 hours after your first login. In this case, you'll skip MFA and go straight to the regular CAFT login page.

## 14. Will I receive an authentication code automatically when I try to log in under MFA?

When prompted for your one-time code during CAFT MFA login, you will need to open the authentication app on your phone and enter the 6-digit code that appears under your CAFT account.

There are MFA systems some users may be familiar with that work by sending a code automatically via SMS-text message or phone call—these systems use a different authentication approach based on users enrolling their phone numbers with the system. However, CAFT MFA is based on the use of a secure authentication app, and you will need to obtain the code from the app when you login.

## 15. How do I know this whole thing isn't a cyberattack like phishing or spoofing?

Phishing is the use of a fake email designed to appear like it's coming from a legitimate source. Spoofing is the creation of a fake web page, also designed to appear as if it's legitimate. Fraudsters use these tools to try and harvest sensitive information like user IDs and passwords.

If you've received an email that is saying it's from Access Credit Union, double-check the email domain (i.e., the part after the @ symbol). It should be @accesscu.ca with no additional symbols or characters. When possible, or if in doubt, confirm the domain against prior communications with us you know to be legitimate.

When logging into CAFT, if you are ever in doubt you've arrived to the right web page, check the link for the CAFT website provided when you initially enrolled into CAFT, or any bookmarks you may have created. You will be able to confirm that you are in the right place by carefully checking the correct URL for CAFT: caft.paymentsanytime.com.

## 16. What if I don't have a mobile device I can use for this?

A mobile device such as a smartphone or tablet is advised so you can download and install one of the recommended authentication apps described in the *CAFT MFA User Guide* you received (also see the FAQ on 'How do I enable MFA?').

If you do not currently have access to a mobile device, obtaining a low-cost smartphone or tablet is one solution. Another alternative is to use the Authenticator Plugin. This is a third-party plugin that installs into Google Chrome or Microsoft Edge browsers and performs the same functions as the aforementioned authenticator apps but within a Web browser.

## 17. What if I'm having trouble getting MFA to work and it makes me late sending in my company's payroll file?

Follow along with your *CAFT MFA User Guide* and the MFA login process should be quick and work without issue. However, to be on the safe side, you may wish to build in as much time as possible ahead of your first transaction after December 6 in case an issue arises that needs to be worked through. For example, if you normally run your payroll transactions late afternoon on a Friday, you may wish to try and run the transaction earlier in the day, or at least attempt to successfully log onto CAFT ahead of time.

## 18. What else should I be doing to prevent fraudulent access to my accounts?

MFA is an important tool for cybersecurity that we are implementing to help keep your information and accounts safe. However, cybersecurity is everyone's responsibility and it is important that we all follow cybersafe practices whenever dealing with sensitive online information.

- *Pay attention to URLs. Ensure you are always using the correct URL for any banking services or other financial transactions that are done online.*
- *Do not communicate or keep a copy of your usernames and/or passwords for any of your financial services (or other secure logins) in your email account. A common way of gaining illegitimate access to a secured account is through the discovery of sensitive information within a compromised email account.*
- *Enable multifactor authentication (MFA) on your email account, if available, for an added layer of security – for example, so you are prompted to enter a security code sent to your phone whenever you attempt to login to your email from a new device.*
- *Be very cautious of unsolicited emails asking for your login credentials and never click on a link to login from an email you were not expecting.*
- *Even if an email appears to be coming from a legitimate sender, if it involves making changes to login or banking information, verify the legitimacy with the sender via another communication method (e.g. phone call).*
- *Always log out of your secure accounts, such as online banking, when using public or shared computers or devices. If possible, avoid using public wi-fi for sensitive activities.*

There are also many good resources on individual and business cybersecurity online. A good one to check out is GetCyberSafe.ca.