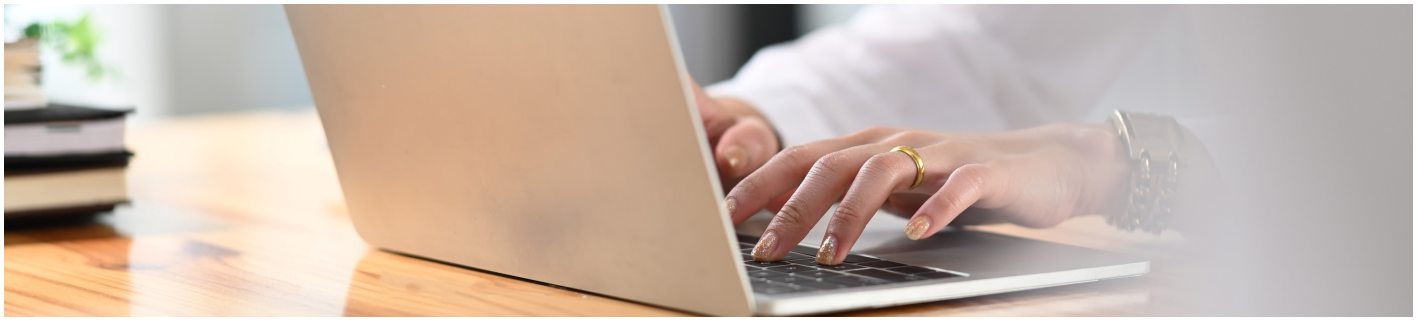
Understanding CAFT



What is CAFT?

Customer Automated Funds Transfer (CAFT) is a web-based solution that allows a business to manage payments. CAFT is compatible with most accounting software and provides the option to enter data manually online.

With CAFT, businesses can initiate:

- Direct deposits like Payroll and accounts payable.
- Collect payments like loans, accounts receivables, strata/ or condo fees, donations and club fees/dues.

CAFT users are responsible to:

- Protect passwords and User IDs.
- Manage CAFT transactions.
- Verify file totals prior to file processing.
- Release files in a timely manner.
- Review CAFT email notifications upon receipt.
- Review the Activity Log.
- Review the History File.
- Verify all NAFT reports.
- Verify account settlement to the settlement register (AFTR0010).
- Contact our team about any changes to Originator information.
- Immediately notify us of any unusual activity.

What You Can do to Protect Yourself

Users can prevent transaction processing due to key error, theft or fraud by:

- Learning about cyber security.
- Implementing internal controls (segregation of duties, dual authorization, setting CAFT limits).
- Reviewing transaction files for accuracy.
- Reviewing CAFT email notifications.
- Reconciling banking transactions daily.
- Talking to insurance provider about Social Engineering coverage.

What do I need to know?

CAFT is a web-based application, therefore Originator accounts could be exposed to cyber fraud if the business or employee's computer system becomes compromised.

If you notice unusual activity:

- Check the CAFT Activity Log and History File information.
- Contact the credit union immediately.
- Change your CAFT password.
- If you have been compromised, follow the security procedures of your company.

Increasing cyber security practices and building fraud awareness are vital in protecting yourself.

Other Best Practices & Resources:

- Create strong passwords and never share your User ID or password.
- Lock or logout out of your computer when unattended.
- Never access bank, brokerage or financial services information using open/free Wi-Fi (e.g. coffee shops, public libraries, hotels, etc.).
- Never click on links or attachments from an unexpected email, even if it looks like it is from a person or organization you know.
- Always use the login page on your browser to login to an account or online service (e.g. CAFT) – never use links in an email.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Ensure virus protection and security software and the operating systems/applications on your computer are updated regularly. Familiarize yourself with the credit union's account agreement and your businesses liability coverage for fraud.

CAFT Features to help Originators mitigate risk

Transaction limit: max dollar value of an individual record.
Mitigates risk by stopping file from processing if transaction limit is exceeded.

File limit: max dollar value of a total file.
Mitigates risk by stopping the file from processing if limit is exceeded.

Daily credit limit (calendar day): max dollar value of file or combined files.
Mitigates risk by stopping file from processing if credit limit is exceeded.

Daily debit limit (calendar day): max dollar value or combined files.
Mitigates risk by stopping file from processing if debit limit is exceeded.

Monthly limit: aggregate of all files sent in a month.
Mitigates risk by sending credit union/financial institution a warning email (note: files will **not** be stopped if the monthly limit is exceeded).

Dual authorization: two users/employees authorize the release of a file.
Mitigates risk by ensuring a second user is reviewing a file prior to releasing.

Sub-Originator limits: groups all files sent on a group of Originators that have been linked together.
Mitigates risk by aggregating all file totals to a maximum daily combined limit. If the daily limit is exceeded, the file will reject.

Email notification: first notification to all email recipients of the file status.
Mitigates risk by warning email recipients of Originator activity.

Pre-settlement: provides the credit union/financial institution the opportunity to pre-settle business member accounts before transactions are delivered (for credit files only).
Mitigates risk by securing funds at the credit union/financial institution prior to settlement (works best with pre-hold option).

Hold late: stops files from processing if released or uploaded to CAFT less than three business days prior to transaction due date.
Mitigates risk by stopping files from processing without the credit union/financial institutions authorization by following their internal authorization procedures.