CAFT User Risk Reference

Tips & Tools

Christian CREDIT UNION

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.

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 your financial institution.
- Change your CAFT password.
- If you have been compromised, follow the security procedures of your company.

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 their financial institutions about any changes to Originator information.
- Immediately notify their financial institution of any unusual activity.

What can I do to protect myself?

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

Other best practices and 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 your institution's account agreement and your businesses liability coverage for fraud.

Find more information at:

- Christian Credit Union
- Get Cyber Safe: www.getcybersafe.gc.ca
- Canadian Anti-Fraud Centre: www.antifraudcentre.ca.