Best Practices for

Your Business

Protecting your organization from Theft and Fraud

FRAUD FACTS

- The Canadian Anti-Fraud Centre received **more than 107,000** reports of fraud in 2021, with losses totalling **$384 million**.[1]
- In 2021, **71%** of organizations were victims of payments fraud attacks/attempts.[2]
- Together, **lack of internal controls** and **override of existing controls** account for nearly half of occupational fraud cases.[3]
- Cheques are impacted by fraud more than any other payment method[4] — but, as more and more business is conducted online, criminals are adapting. **Cybercrime is rising rapidly**, and the number of police-reported cybercrime incidents in Manitoba has nearly tripled since 2017.[5]
- Think your business won't be impacted by fraud? Think again! The risk of fraud is **always present** and **always changing**.
- Fraud can result **in lost revenue and time** for your business.
- **Customers may also be impacted** if services are interrupted or their confidential information is compromised.

Fraud can hurt your reputation and your bottom line, but there are steps you can take to protect your business.[6]

Stay Vigilant. Stay Safe

1 Government of Canada Anti-Fraud Centre, December 2022
2, 4 Association for Financial Professionals®: 2022 Payments Fraud and Control Survey
3 Association of Certified Fraud Examiners: Occupational Fraud 2022: A Report to the Nations®
5 Statistics Canada, December 2022
6 For more information, tips and advice, visit **Competition Bureau Canada > Fraud and Scams**

fusion credit union

Best Practices

Deposit Accounts

Review statements regularly. Have your business's banking statements sent directly to your personal email or home address, and review them regularly and in detail.

Limit access to credit and debit cards. The more employees with company cards, the greater the chance of fraud. Require employees to document all business expenses with detailed receipts, and review all credit and debit card statements for accuracy.

Monitor point-of-sale transactions and count cash at the beginning and end of each day. Use point-of-sale software that requires employees to log in, identifying who is on the register at any given time.

Don't put one person in charge of petty cash. Require a second employee to authorize all transactions. Record all transactions and balance the petty cash every week.

Review all outgoing payments and compare to invoices. Watch for duplicate invoices, new vendors or multiple invoices from the same vendor in a short time — embezzling employees often use these tactics to pay themselves.

Require vendors to submit detailed invoices. Avoid vague language on invoices.

Sign cheques yourself. Require all cheques and payments to be signed or authorized by the business owner or established signing authorities. Do not pre-sign cheques.

Review payroll before it's processed. Watch for variations in amounts and use direct deposit to reduce risk of fraud.

Store the cheque book safely. Notify the credit union immediately if cheques are missing.

Segregate duties. Employees who sign cheques should not be completing reconciliations.

Establish signing authorities and implement dual signature requirements. Notify the credit union of any change in signing authority or organizational structure.

Don't be predictable. Keep the element of surprise on your side when watching for employee misconduct, by performing financial reviews and audits at random times.

Have an external auditor review your business's financials, for an independent and unbiased perspective.

To learn more about how to protect your business from fraud, visit **fusioncu.com/en/business/support**

PROTECT YOUR PERSONAL INFORMATION

Fusion Credit Union will NEVER ask you to provide personal and confidential information (such as logins, passwords, authentication codes) by phone or email

Best Practices

Small Business Online Banking

Use strong passwords and keep them secret

- Use long passwords with a combination of letters, numbers and special characters.
- Create unique passwords for each website login and email account.
- Do not share passwords or login credentials. Each user should have an assigned username and password.

Segregate duties

- Delegate access and authorize signers based on employee responsibilities, and ensure adequate segregation of duties involving custody, authorization and control of source documents and records.
- Dual authorization requires two individuals to complete a transaction — no individual should have sole authority to initiate or authorize a transaction.

Advise Fusion of changes to signing authorities & delegates

- Provide updated resolutions regarding changes in signing authorities so access to digital banking can be updated.
- Digital Banking access is granted to the individual and does **not** distinguish by position or assigned authority. While an organization's rules may state, for example, that "Two signers are required, one of Mayor or Deputy Mayor AND one of CAO or Assistant CAO," Fusion Credit Union requires the name of each individual.
- Delegates are managed by authorized signers of the account with Digital Banking access — changes to staff employment or authority should be managed immediately.

Establish Internal Controls and review them regularly

- Strong internal controls (policies, processes and procedures) will not make your company immune to fraud, but they can make it less attractive as a target to both internal and external fraudsters looking for weaknesses to exploit.
- Internal controls are a set of tools that evolves over time as the business, technology and fraud environment changes. Fusion Credit Union can help ensure you're employing best practices — contact your branch manager for more information.

Protect your computers

- Install anti-virus and malware on your business computers and/or network, and keep it up to date.

Register for Interac e-Transfer Autodeposit

- Autodeposit is a secure way to accept e-Transfer payments without having to answer security questions, reducing the risk of fraud.

Educate employees about fraud prevention

- Keeping employees up to date on how to avoid fraudulent schemes will not only protect your business — it will also equip your staff to educate customers, to everyone's benefit.

Robust, up-to-date internal controls are the best defence for your business against both cybercrime and employee theft.

Fusion Credit Union can help — ask your branch manager for more information.

fusion credit union

Best Practices

Wire Drafts

- Independently confirm wire transfer requests using contact information on file, or from website or directory (**not** from the email or fax instructions). Transactions should be authenticated with **every** request, using identifying questions and transaction history.
- Review each request carefully, watching for slight changes to an email address, spelling, grammatical errors, a high sense of urgency, unavailability of the recipient, international transfers, high dollar amounts, and increased frequency.
- Do not rely only on the history of similar email wire transfer requests, as a fraudster may have intercepted that correspondence with the purpose to introduce similar but fraudulent transactions.
- Educate employees on the dangers of opening attachments or clicking on links in unsolicited emails, and delete sensitive information.
- Use strong passwords and keep anti-virus and anti-malware software up to date.
- Avoid sending sensitive emails using hotspots.
- Do not allow employees to access personal emails on work computers, or browse the Internet freely on the same computer used to initiate payments.
- Never leave USB drives in computers used to connect to payment systems.
- Monitor employee logins outside of normal business hours.

Best Practices

CAFT Customer Automated Funds Transfer

- Educate employees about cyber security.
- Implement internal controls (segregate duties, dual authorization, set CAFT limits).
- Require all requests to change payee/ payor account information received via email to be confirmed by phone using the contact number on file (**not** the number included in the email request).
- Review all transaction files for accuracy.
- Review all CAFT email notifications.
- Reconcile banking transactions daily.
- Consult your insurance provider about Social Engineering coverage.
- Create strong passwords and never share your User ID or password.
- Lock or log out out of your computer when unattended.
- Never access bank, brokerage or financial services information using open/free Wi-Fi (at coffee shops, libraries, hotels, etc.).
- Never click on links or attachments from an unexpected email, even if it looks like it came from a person or organization you know.
- Always use the login page on your browser to sign in to any account or online service, including 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, security software and the operating systems/applications on your computer are updated regularly.
- Familiarize yourself with Fusion Credit Union's account agreement and your businesses liability coverage for fraud.

To learn more about how to protect your business from fraud, visit **fusioncu.com/en/business/support**