Fraud Prevention – Tip Sheet

Strategic Tips to Help Minimize Fraud Risk

The risk of business fraud today is higher than ever. Businesses are constantly threatened by new innovations in fraud. Criminal networks are often global in scale, they are persistent and creative in designing schemes intent on gaining access to information. It is becoming more challenging for businesses to monitor the increasingly sophisticated fraud tactics of criminals.

Fraud can have a serious impact on both your business' reputation and its finances so it is essential to be familiar with the emerging fraud trends, and take the right steps to help protect you and your clients. Remember, at CIBC, we will never send you an email requesting your banking information. Here are a number of fraud trends and warning signs to help detect and prevent possible fraud occurrence.

Emerging Fraud Trends

Social Engineering: Business Compromises

Social engineering is the act of manipulating people into performing actions or divulging confidential information. Criminals are adept at using the Internet, email and phone to target businesses for the purposes of committing fraud. Increasingly, criminal attacks are targeting specific roles and individuals who have access to critical information.

During the past year, "Business Email Compromise" and "Impersonation" have become more prevalent. Criminals are contacting companies and impersonating executives, employees, vendors or third parties to request a payment, transfer of money or change existing payment instructions. Some of these emails are difficult to identify because they may include information that makes them appear authentic.

Warning Signs:

- Urgent Tone
- Ad Hoc Payment Requests
- Incorrect Email Address
- Poor Spelling or Grammar
- Requests from Free Email Accounts

Malicious Software

Users of online banking services in Canada and around the world are regularly targeted by fraudsters using malware. Malware, short for malicious software (also known as a computer virus), can be used to provide fraudsters with remote access to your computer and information to conduct fraudulent activities without your knowledge.

Warning Signs:

- Unfamiliar screens or popups on websites/ applications
- Slower or abnormal computer performance
- Fraudulent messages on Cash Management Online (CMO) sign on screen
- Unexpected calls from someone pretending to be "the bank" asking for confidential security information

How to take Protective Measures

Staying informed is the first line of defense against becoming a fraud victim. The following preventative measures and best practices will limit you and our clients' fraud risk exposure against common fraud attempts.

Preventative Measures:

- Think before you click: Do not open email attachments or click on links from senders you do not know
- Be suspicious of unfamiliar screens or request from websites/applications that you regularly use
- Verbally confirm any financial transactions, including changes to payment instructions, requested by e-mail using a known phone number and don't respond to any number left on phone or fax instructions
- Have a dual approval process for financial transactions
- Use secure remote access methods
- Establish role-based access controls and implement system logging and dual approval on payments
- Protect your confidential Information and never reveal your PIN to anyone
- Use passwords that have a combination of upper case letters, numbers and special characters
- Implement an employee cybersecurity and fraud training program
- Implement measures for detecting compromises and develop a cybersecurity incident response plan

Best Practices

- Review the message board on CIBC Cash Management Online for updates
- Keep anti-virus and anti-malware software up to date
- Backup systems regularly Ensure employees are trained to recognize fraud, and what to do if they become a victim
- Ensure employees know what policies, processes & controls are in place
- Contact the Business Contact Centre immediately for any wires that you believe are fraudulent
- Reconcile bank accounts daily
- Safeguard cheque stock and eliminate "windowed" envelopes for mailing cheques
- Recommend clients to reduce/eliminate cheque issuance and move more to electronic means of receiving and distributing cash with Payment Solutions such as CIBC's Cash Management Online, or leverage services such as Positive Pay where a business need for cheques & utilize Email Alerts

Additional Considerations

- Review & update System Security & Firewalls
- Review & update regularly Cybersecurity Plans & Procedures
- Review and update Response Plan components i.e. action plan / roles and responsibilities

For more information on fraud prevention, contact the CIBC Business Contact Centre Technical Support team at 1 800 500-6316 or visit CIBC.com Privacy & Security Policy.