Fraud Prevention Best Practices

www.rbc.com/cyber/business

Allison Cathcart & Cherie Nykolaichuk

June 2026

RBC Commercial Financial Services Team

Andrew Staniforth

Vice President, Agriculture
andrew.staniforth@rbc.com
613-218-1100

Tracy Young

Senior Relationship Manager, Agriculture
tracy.young@rbc.com
613-203-4770

Allison Cathcart

Commercial Banking Advisor
allison.cathcart@rbc.com
289-404-2680

How the Fraud Landscape is changing

The frequency and complexity of fraud and scams has increased significantly in recent years. Fraudsters are continually evolving their schemes and using Artificial Intelligence and advanced technology together with social engineering tactics.

Artificial Intelligence (AI) and sophisticated technology

Advances in AI and technology make it harder for businesses and their employees to recognize frauds and scams

Social Engineering Tactics

Social engineering tactics, such as impersonation schemes, are used to bypass traditional and internal fraud controls. They manipulate businesses into sharing confidential information. This includes the sharing of log-in credentials and passwords

Scam vs. Fraud

What is the difference between scam and fraud?

A scam is a dishonest scheme or trick intended to deceive or manipulate individuals or businesses. This is to obtain money, information, or access.

Fraud is the criminal act of obtaining money, property, or services through deception. Fraud often occurs as a result of a successful scam.

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Business Email Compromise is a scheme where a fraudster impersonates an employee of the company, to gain information or steal from the company.

By using the existing relationship, the fraudster tricks the recipient of the email into sending money or sharing information.

Requests typically include an element of urgency and a request for confidentiality. The requests are well-worded, specific to the business being victimized, and do not raise suspicions as to the legitimacy of the request.

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Vendor Email Compromise targets businesses with well established relationships with their suppliers, contractors, and even employees.

The email often includes new banking information together with instructions to send future payments to a new account, which belongs to the fraudster.

An example of this would be when a fraudster uses a compromised email to inform of a change of payment details.

Allison@mylocalfair.ca	correct email
Alison@mylocalfair.ca	wrong email

or……..

office@anylocalfarm.ca	correct email
office@anylocalfarms.co	wrong email

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Wire Transfer

This type of fraud occurs when a fraudster tricks the individual or company into sending money to their bank account under false pretenses, usually through impersonation methods.

The requests for wire transfers are well-worded, specific to the business being victimized, and do not raise suspicions

The best defence is to verify before you send. One phone call can prevent significant financial loss

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Fake Invoicing

This is used by fraudsters to request money from a business for a service that they never agreed to.

Invoicing could also be noted as “past due” to increase the urgency of payment without the usual checking of information.

The scammer will keep any money that is sent to them.

Controls can be put in place to stop these scams from happening.

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Remote Access Fraud

This occurs when fraudsters gain unauthorized access to computers or other devices through a fake site or link, while pretending to be a legitimate company.

Once on the system, they will steal passwords to move money.

If anyone asks for access to your computer, treat it as a potential fraud until you can independently verify who they are.

Fraudsters have been busy shifting their focus by refining and targeting their attacks for greater financial return, through these common tactics:

Business Email Compromise

Vendor Email Compromise

Wire Transfer

Fake Invoicing

Remote Access Fraud

Bank Impersonation Scam

Bank Impersonation Scam

This scam often starts with a phone call, text or email from someone posing as a bank employee.

They may use the name of a bank employee that you are familiar with when they reach out to you. They will claim your account has been compromised and they will ask for passwords, PIN's, or verification codes to access your information.

**Banks will never ask for passwords or PIN's. Hang up and contact your bank directly.

Recourse Timeframes

- Canadian Payments Association
  - CPA rules
- Recourse timeframes
- Hold policy

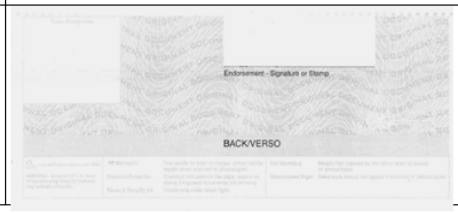
Type of Cheque Fraud	Return Time Limit
Forged Drawer's signature	Next Business Day
Counterfeit	Next Business Day
Material Alteration	Up to and including 90 calendar days
Duplicate Presentment	Up to and including 90 calendar days
Forged Endorsement	6 years
Intended Payee Not Paid	6 years

Cheque Fraud

Did you know that there are 5 types of Cheque Fraud?

	Example	Definition, Recourse and Process
Forged Maker Signature (also known as **Forged Drawer** or **Forged or Unauthorized Signature**)		A forged drawer / maker signature has a forged signature on the front of the cheque. *CPA Rule A4 #2(e)* ***It can only be returned via the clearing system the following business day.*** *CPA Rule A4 #5* If RBC is not notified within the return period / deadline, the funds will be retrieved on a **best efforts basis**. You will be required to complete a statutory declaration if recourse via the clearing system has been lost.
Counterfeit Item		A counterfeit cheque is an item that appears to be an original but has been fraudulently made. *CPA Rule A4 #2(a)* ***It can only be returned via the clearing system the following business day.*** *CPA Rule A4 #5* If RBC is not notified within the return period / deadline, the funds will be retrieved on a **best efforts basis**. You will be required to complete a statutory declaration if recourse via the clearing system has been lost.
Material Alteration		A materially altered cheque is an unauthorized change to an original cheque, such as the Payee, sum payable, or date. *CPA Rule A4 #2(i)* ***It can be returned via the clearing system within 90 days of receipt by the Drawee where supported by a cheque maker declaration.*** *CPA Rule A4 #6(f) & #15* *Note: If returned within following business day (CPA Rule A4 #5), no declaration required. If Negotiating Institution requests declaration after return received, Drawee shall make a reasonable effort to provide. CPA Rule A4 # 15 (b) & (c)* Contact your AMCS*. Complete a declaration and the cheque will be returned through the clearing system. All items reported outside the recourse period will be done on a **best efforts basis** via correspondence.

Daily Reconciliation is key – in some cases there is only 24 hours to report cheque fraud

Forged Endorsement		A forged endorsement is a cheque with a signature on the back that appears to be the Payee but is not. *CPA Rule A4 #2(d)* ***It can be returned via the clearing system within 6 years of receipt by Drawee, where supported by a Payee declaration.*** *CPA Rule A4 #6(a) & #15* Contact your AMCS*. Payee must complete the declaration form and remit it as soon as possible so the process can be initiated.
Intended Payee Not Paid (missing endorsement supported by payee declaration)		Intended Payee Not Paid is the return reason for cheques where an endorsement is missing and the named & intended payee(s) is claiming non-receipt of the funds. (Please note: This does not include altered payee items.) *CPA Rule A4 #2(h)* ***It can be returned via the clearing system within 6 years of receipt by Drawee, where supported by a Payee declaration.*** *CPA Rule A4 #6(g) & #14 Alternative 1* Contact your AMCS*. Payee must complete the declaration form and remit it as soon as possible so the process can be initiated.
Missing Endorsement Not Supported by Payee Declaration (only via correspondence)		A cheque with a missing endorsement has not been signed on the back by the intended Payee(s). ***If not supported by a Payee declaration, it cannot be returned via the clearing system and must be addressed via correspondence only.*** *CPA Rule A4 #14 Alternative 2* Contact your AMCS* as soon as possible so the process can be initiated.

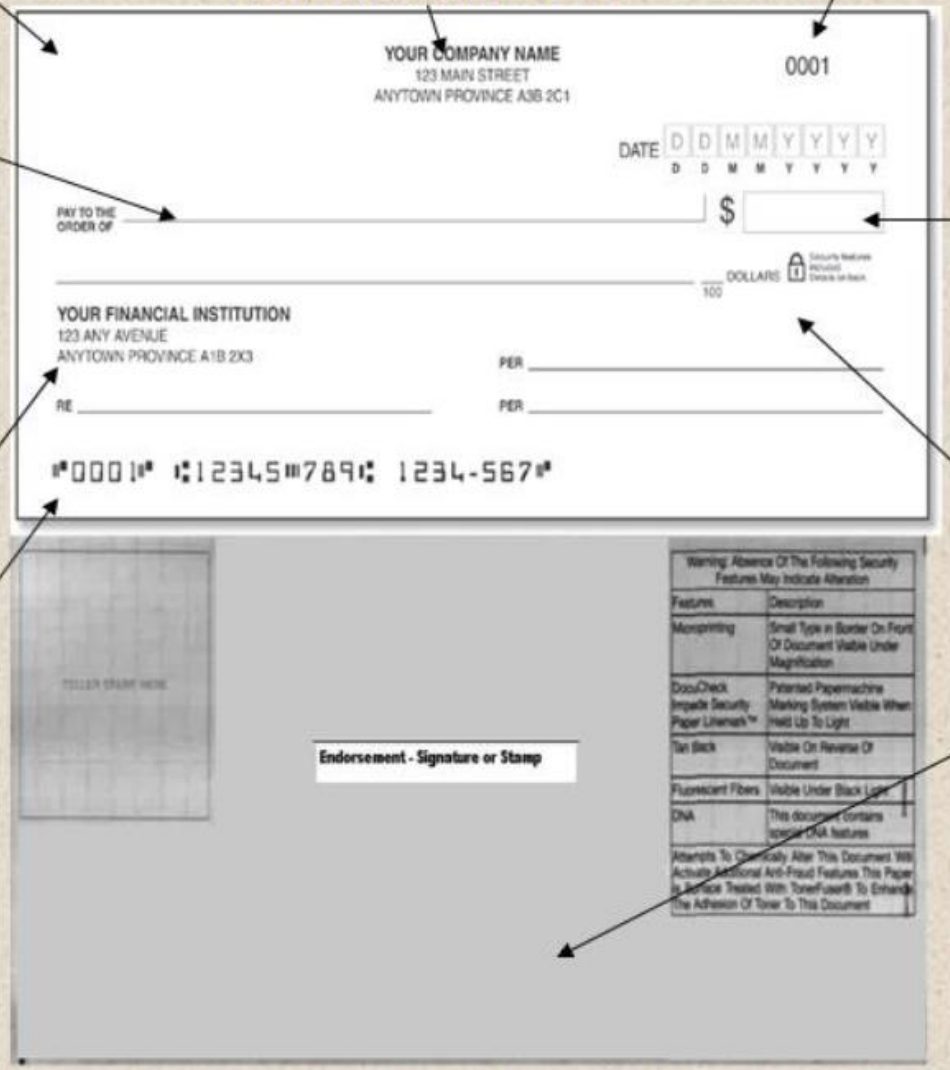
Characteristics of a Counterfeit Cheque

Border & Background:
Does the border & background of the cheque match the client's regular cheques?

Address and Phone:
Do they match the Companion cheque & the clients SRF information?

Serial Number:
Does it make sense given the client's history?

Payee:
Has the Payee been paid before? Is the Payee related? Does the Payee make sense for the client? Does the address of the payee make sense for the location and business of the Payor? Is this a "High Risk" Payee such as a FI or MSB?



Amount:
Is it in range of the client's regular activity? Is it aimed below a possible threshold? (Examples; 4985.00 or 9851.68)

Security Features:
Are they consistent with the client's regular cheques?

Font size and style:
Are they consistent with the client's regular items?

Back:
Is the back of the item consistent with the client's regular cheques (the existence and location of the endorsement line, teller stamp box and any security features on the back)?

MICR Line:
Was the MICR Line stripped (re-encoded)?

How to protect yourself

You play an important role in safeguarding and protecting your systems, devices, and accounts

- Enable on-line security features on all on-line accounts. This includes two or multi-factor authentication. This adds an extra layer of security
- Only download software from a reputable websites, ensure firewalls, anti-malware and anti-virus software are up-to-date and scan PC's regularly
- Reconcile your bank account daily and report any suspicious transactions
- Do not disclose banking credentials including Sign In ID, password or token values
- Do not click links, download files or open attachments from an unknown senders
- Confirm all changes with a call to the vendor's phone number in your files – never from the instruction itself
- Verify the source of all payment requests and validate all invoices before making payments
- Exercise extra caution if you receive email requests for urgent payments or whenever you are suspicious of the payment instruction

How to protect yourself

You play an important role in safeguarding and protecting your systems, devices, and accounts

- **Use Strong Security questions**. Ensure that your questions are difficult to guess. Avoid answers that can be found easily through social media. This also applies to security questions for e-transfers. Never include the answer to a security question in the message of the e-transfer.
- **Use a secure internet connection**. Stay off public wi-fi. Especially when accessing account information. Public wi-fi is a common target for fraudsters.
- **Use strong, complex passwords**. Passwords should be long, contain upper and lower case letters, numbers and special characters, which can include spaces. Storing your password securely is also critical to protecting your digital life. Use a secure password manager.
- **Don't forget about physical security of devices**
  Don't leave in cars. Ensure screens are locked when you're not working

Protect yourself and your loved ones

Protecting ourselves from fraud is more important than ever. Here are some tips to **safeguard your financial security and share with your colleagues, teams, clients, family and friends:**

Break the Spell

• Press Pause – don't be in a rush to share information or complete any action, even if it's someone you know asking to send the payment
• Think Twice – does the request make sense? Do your research!
• Phone a friend – call someone you can trust, either a loved one, friend, colleague or the bank or organization purportedly on the other end of the line

Remember, RBC will NEVER:

• Ask you to disclose your PIN – do not share your PIN with anyone!
• Ask you to share security or verification codes (including one-time passcodes)
• Ask you to disclose answers to your Personal Verification Questions

Friendly Reminders:

• Install RBC Mobile Banking App and adopt it over Online Banking
• Set up Mobile Banking alerts and notifications (click here to learn how)
• Set-up Multifactor Authentication (click here to learn how)

Canadian Anti-Fraud Center

[Canadian Anti-Fraud Centre (antifraudcentre-centreantifraude.ca)]

Phone number 1-888-495-8501

Little Black Book of Scams

[The Little Black Book of Scams 2nd edition (canada.ca)]

Other resources

Additional external links to public websites:

https://cba.ca/protecting-canadians-from-fraud
https://cba.ca/?tag=scams
https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/2024CyberSecurityOlderAdultToolkitUpdated_EN.pdf
https://www.consumerreports.org/gift-cards/how-to-avoid-gift-card-scams/
https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards
The Little Black Book of Scams 2nd edition – *now available in 8 different languages!*

What to do if you are a Victim

Report, Report, Report!!!

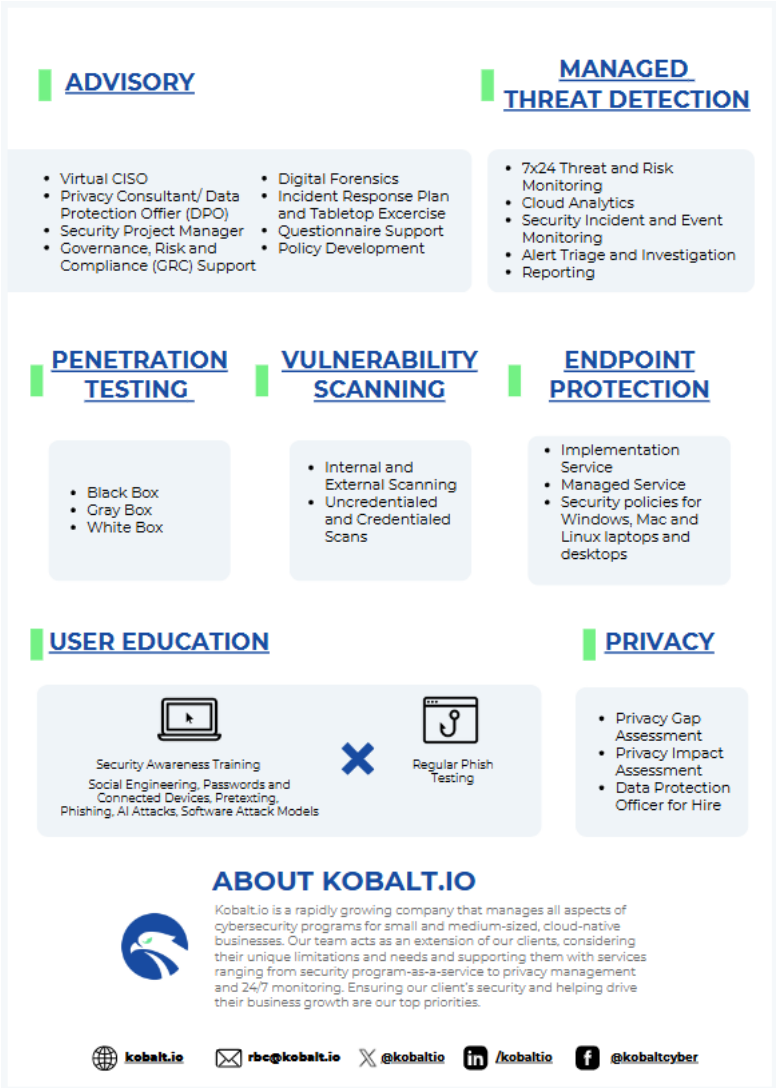
- Contact your bank
- Contact the police
- Contact the Canadian Anti-Fraud Centre
- Get your systems and devices cleaned by a professional
- Change your passwords
- Close the compromised account
- Increased controls

Beyond Banking

Special access to our partners and their offers for your business

From simplifying your business, to attracting customers, to building and retaining talent and managing your cash flow, our evolving list of partners is available to support you wherever you are in your journey. Services Beyond Banking - RBC Royal Bank

Beyond Banking



Thank you
for attending

Questions?

How RBC keeps you safe

- Strict privacy policies
- Investment in new technologies
- 24/7 fraud experts
- 100% Online Security Guarantee*
- Education

Find out RBC's guarantee to you:
RBC Secure Banking Guarantee - RBC Royal Bank

* For a definition of an unauthorized transaction and for full details regarding the protections and limitations of the RBC Digital Banking Security Guarantee, please see your Electronic Access Agreement for personal banking clients, and the Client Card Agreement and the Master Client Agreement for business clients. This guarantee is given by Royal Bank of Canada in connection with its Online and Mobile Banking services. Cardholders are not liable for losses resulting from circumstances beyond their control provided they have taken reasonable precautions to protect their Client Card and PIN (if applicable) as set out in the Client Card Agreement. Formerly known as the RBC Online Banking Security Guarantee.

Disclosures:

The strategies, advice and technical content in this presentation are provided for only general guidance to benefit our clients. This presentation is not intended to provide specific financial, investment, tax, legal, accounting or other advice for you, and should not be relied upon in that regard. Readers should consult their own professional advisor when planning to implement a strategy to ensure that individual circumstances have been considered properly and it is based on the latest available information.