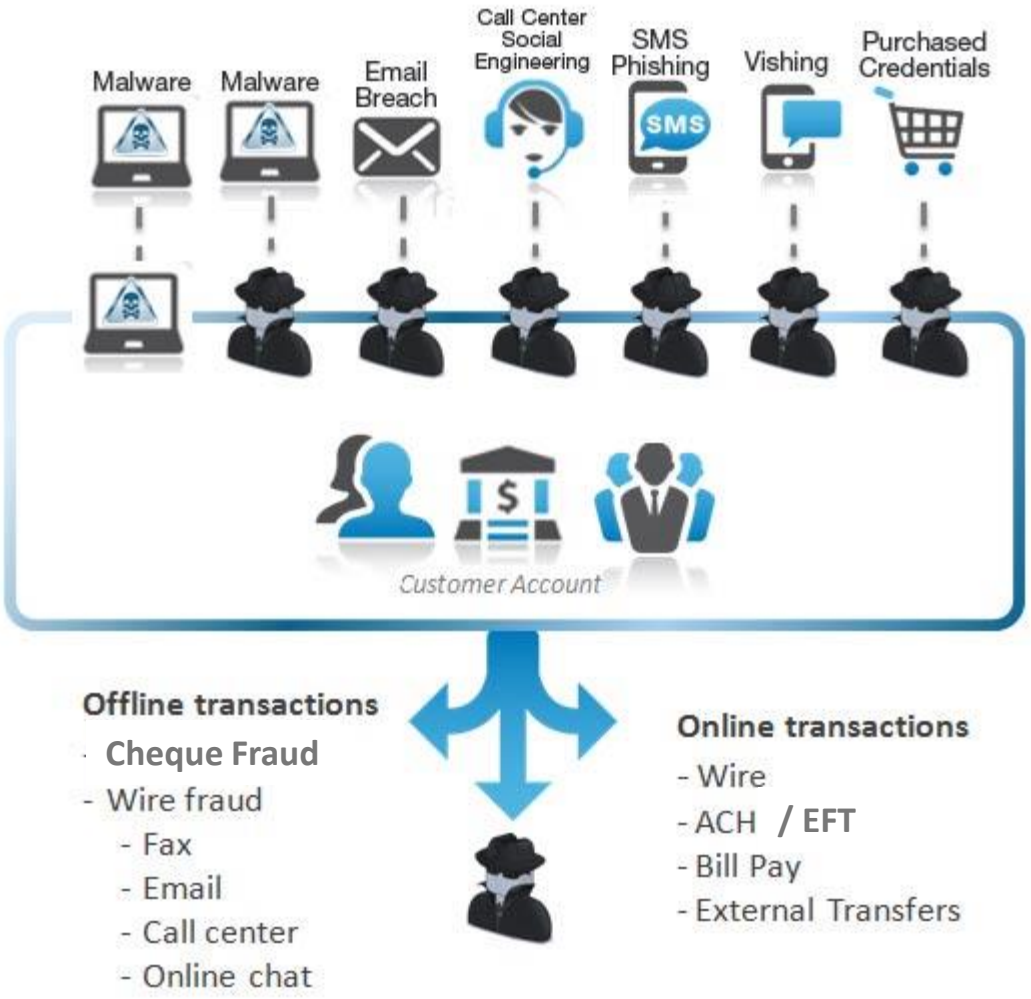
Fraud & Security

An Overview – from a banking perspective

September 28, 2017

Scotiabank

Fraud Exploit Paths



Scotiabank

Business Email Compromise

- Business email compromise (BEC) scams are a type of payment fraud that involves the compromise of legitimate business email accounts for the purpose of conducting an unauthorized wire transfer.
- In the cases of email fraud, your vendor's or your own employee's email is hacked in order to request the wire payment.
- You initiate a wire payment through Scotia Connect believing you are paying a legitimate vendor.
- Your employee does not verify the legitimacy of the email instructions with the vendor/employee prior to sending the wire payments.
- You do not detect that the email instructions are fraudulent until after multiple payments have been sent.

Business Email Compromise – CEO Scam

- The business email account of an executive is compromised. This is achieved through malware or social engineering.
- The scammers research the executives, check travel schedules and read other business emails through the compromised email account
  - Criminals send emails concurrently with business travel of the executives whose emails are compromised, making the emailed request seem more plausible and more difficult to verify.
- An employee at the compromised company receives an email request to transfer funds, seemingly from the executive at their company
- The employee believing the email to be legitimate, transfers the funds to the criminals
- Businesses and employees using open source email are the most at risk for business email compromise scams. In many cases the criminals spoof emails of individuals within enterprises who are authorized to submit payment requests and then send them to employees with the authorization to process them.
- Employees who handle wire transfers are often **targeted**

Spoofed E-mail accounts

- Spoofed – when a criminal is trying to trick you into thinking that they are coming from a legitimate account
  - Headers are spoofed so it looks completely legitimate upon receipt
  - Only when you “reply” can you see it is a completely different email address

Electronic Funds Transfers (EFT)

- Your vendor requests to change their bank account details
- The fraudster sends a email pretending to be your legitimate vendor requesting to update their Bank account information.
  - jsmith@vendorcompony.com instead of jsmith@vendorcompany.com
- The payment change is processed by your well intentioned employee
  - No attempt made to confirm the validity of the request.
- The next time your legitimate vendor issues an invoice to you, the funds are redirected to the fraudster's Bank account as a result of the fraudster being able to update the Bank account information.

How do fraudsters gain access to sensitive payment systems?

Phishing

- “Phishing” is a type of identity theft where criminals use email to try to bait you into fake websites. Once there, you are asked to disclose confidential financial and personal information, like passwords, credit card numbers, access codes or Social Insurance Numbers. The most familiar type of phishing scam is an e-mail threatening serious consequences if you do not log in and take action immediately.
- Never respond to emails, open attachments, or click on suspicious links from reputable institutions or unknown senders asking for personal or financial information.
- Always remember that Scotiabank will never send you unsolicited emails asking for confidential information, such as your password, PIN, Access Code, credit card and account numbers. We will never ask you to validate or restore your account access through email or pop-up windows.
- If you have entered personal information after clicking on a link or suspect fraudulent behavior, please call us immediately at 1-800-4-SCOTIA (1-800-472-6842).

Cyber Attacks

Attack Type	Definition
Distributed Denial of Service	▪ Attempts to flood bank websites with traffic to make it unusable for normal customer access.
Web Attacks	▪ Attacks against the web application code to circumvent controls and steal information.
Infrastructure Attacks	▪ Attacks against the bank's network to circumvent controls and provide hackers with remote access.
Client-Side Attacks	▪ Malware and viruses which circumvent the security controls of a client workstation to perpetrate fraud.
Social Engineering	▪ Attacks against employees by imposters pretending to be legitimate banking customers.

Fraudsters can compromise new technologies but….

…….Cheque Fraud is still alive and well

Scotiabank

Common Types of Cheque Fraud

Cheque Type	Definition	CPA Return Time frame
Counterfeit Cheque	▪ Counterfeit cheques generally have slight differences compared to legitimate cheques. The color, logo, font, security features may vary.	24 hours
Altered Cheque	▪ Materially altered cheques are valid and authorized items, but contain changes to the payee's name; date; amount (figure/words); time of payment.	90 days
Forged Signature	▪ Signature on the face of a cheque that is not the signature of the authorized signatory or signature that is written on or applied to an item without the drawer's authority.	24 hours
Forged Endorsement	▪ Forged Endorsement is a situation when a cheque is endorsed and cashed by another unauthorized individual, other than the intended payee.	6 years
Intended Payee not Paid	▪ Cheque can be returned with the reason Intended Payee Not Paid, when the cheque is negotiated by another unauthorized party, other than the intended payee.	6 years
Duplicate Presentment	▪ Fraud made possible through new digital deposit channels such as Mobile and Business. Individual or entity deposits an image through the digital channel one or more times, after which the item is presented through an alternate channel in paper form such as an ABM, Branch, Night Deposit.	90 days

Positive Pay and Positive Pay with Payee Match

- **Positive Pay** enables customers to stay on top of their cheque processing, with scheduled Paid Cheque and Outstanding Issued file transmissions, and online cheque image, search and reporting features. With our **"Negative Pay"** feature, customers can conveniently return cheques online.
- The benefits of this Positive Pay are realized by every market segment - the larger the market segment, the greater the time savings, making it ideal for businesses with 250 or more cheques per month and/or an in-house cheque-based payroll.
- **Positive Pay Service with Payee Match** is a comprehensive fraud detection service that provides customers with all of the fraud protection features of Positive Pay (serial number, amount, and issued versus clearing date verification) and the added protection of Payee Match, which includes the ability to detect alterations to the payee information of a clearing cheque

How Can You Protect Yourself and Your Company

Best Practices for Fraud Prevention

- Daily Reconciliation – Reconcile all your business banking transactions daily.
- Month-End Bank Statements – Review every item on your statement, including cheque images.
- Centralize Your Cheque Issuing – Do not leave cheques available to unauthorized staff.
- Lock Up Cheques – Securely and separately lock up unissued cheques, facsimile signature stamps and any cheque reorder forms.
- Bill Payments – Complete routine bill payments electronically. Internet banking services can facilitate post-dated payments.
- Tax Payments – Pay GST/HST/TVQ and other tax payments on a Web-based tax payment and filing service.
- Credit Cards – Encourage suppliers to accept credit card payments for purchases under $5,000 to eliminate small-dollar cheques.

Best Practices for Fraud Prevention (con't)

- Payroll Cheques – Link your in-house computer payroll software to an Electronic Funds Transfer (EFT) Service to provide direct deposit to employee accounts.
- Pre-Authorized Payments – By authorizing your creditors to automatically debit your account for payments.
- Deposits – Direct deposits to a central deposit account and verify activity daily.
- Separate the Functions – Different people should be responsible for the writing and/or signing of cheques, and the reconciliation of the bank statements and electronic payments.
- Special Accounts – Open separate accounts to separate such functions as incoming wires and high-volume small-dollar cheques.
- Security Audit – Obtain a full audit by an accounting professional that includes a complete review of your security procedures.
- Insurance – Review your coverage regularly.

Safe Computing Practices

- Protect Your Privacy
- Download Free Rapport Security Software
- Use Anti-Virus Software
- Protect Your Internet Connection
- Use Supported Browsers

Please click on the website below for further information on the above topics

http://www.scotiabank.com/ca/en/0,,2973,00.html

Be Prepared

- Be Prepared to Isolate Any Compromised Systems
- Know Your Legal Counsel
- Consider Where You Need Help
- Build Your Communications and Strengthen your Fraud Awareness
- Train Employees Accordingly
- Continue to think before you click
- Keep locking up
- Continue to use common sense and nurture your inner skeptic
  - Your bank will never call and ask you for your PIN or online banking password. The old adage is true: if it sounds too good to be true, it probably is.