Best Practices in Fraud Prevention

Pamela Kelly
TD Commercial Banking

The Payments Fraud Landscape

- 62% of organizations surveyed experienced attempted or actual payments fraud.
- 28% of survey respondents reported that incidents of fraud increased over previous years.
- 77% of organizations that experienced attempted or actual payments fraud were victims of cheque fraud
- Cheques remain the most-often targeted payment method by those committing fraud attacks. Cheque fraud also accounts for the largest dollar amount of financial loss due to fraud.
- 27% of organizations surveyed experience attempted/actual wire fraud (nearly double previous years)
- 25% of organizations surveyed experienced attempted/actual EFT fraud

** Source: 2015 AFP Payments Fraud and Control Survey*

Cheque and Mail Fraud

- Although the use of cheques is decreasing, it continues to be the #1 type of payment fraud
- Available technology (scanners, printers, etc.) makes cheque fraud easy to commit
- Companies should carefully manage cheque stock and explore cheque alternatives such as electronic payments (EFT)
- Cheques mailed in window envelopes continue to be a key target for mail fraud – consider using regular envelopes and/or special cheque printing with the cheque folded inside
- Protect your account information – store paid cheques on DVD instead of on paper; do not provide your chequing account number to your customers; protect your internal systems and records

Trends in online fraud

- **Phishing**
  - An authentic-looking email appearing to be from a legitimate company
  - Often asks for your personal or financial information
- **Malware (“malicious software”)**
  - It is possible to download malware without realizing it, from:
    - A link in an email
    - A “poisoned” link on a search engine or social media site
  - Whatever the source of infection, once malware is loaded on your PC, your **information and login credentials are at risk**
- **Email Takeover**
  - Increasingly, people are being duped into accepting **fraudulent payment instructions** via email
- **Ransomware**
  - a type of malicious software designed to block access to a computer system until a sum of money is paid.

Protecting Your Organization

- **Education**
  - **Be aware** of the most common types of fraud and share knowledge with others in your company
    - Look for signs that an email or phone call is not legitimate
    - Exercise caution - pop-ups or messages may be a sign of malware – call your Bank immediately if you suspect your PC is compromised
  - Understand what you can do to **protect yourself**, as well as what your bank can do to help
  - Encourage a **climate of transparency & empowerment** - all employees should feel free to question instructions
- **Detection**
  - Monitor accounts and audit logs daily – contact your branch or the help desk if you can't access your service

Protecting Your Organization

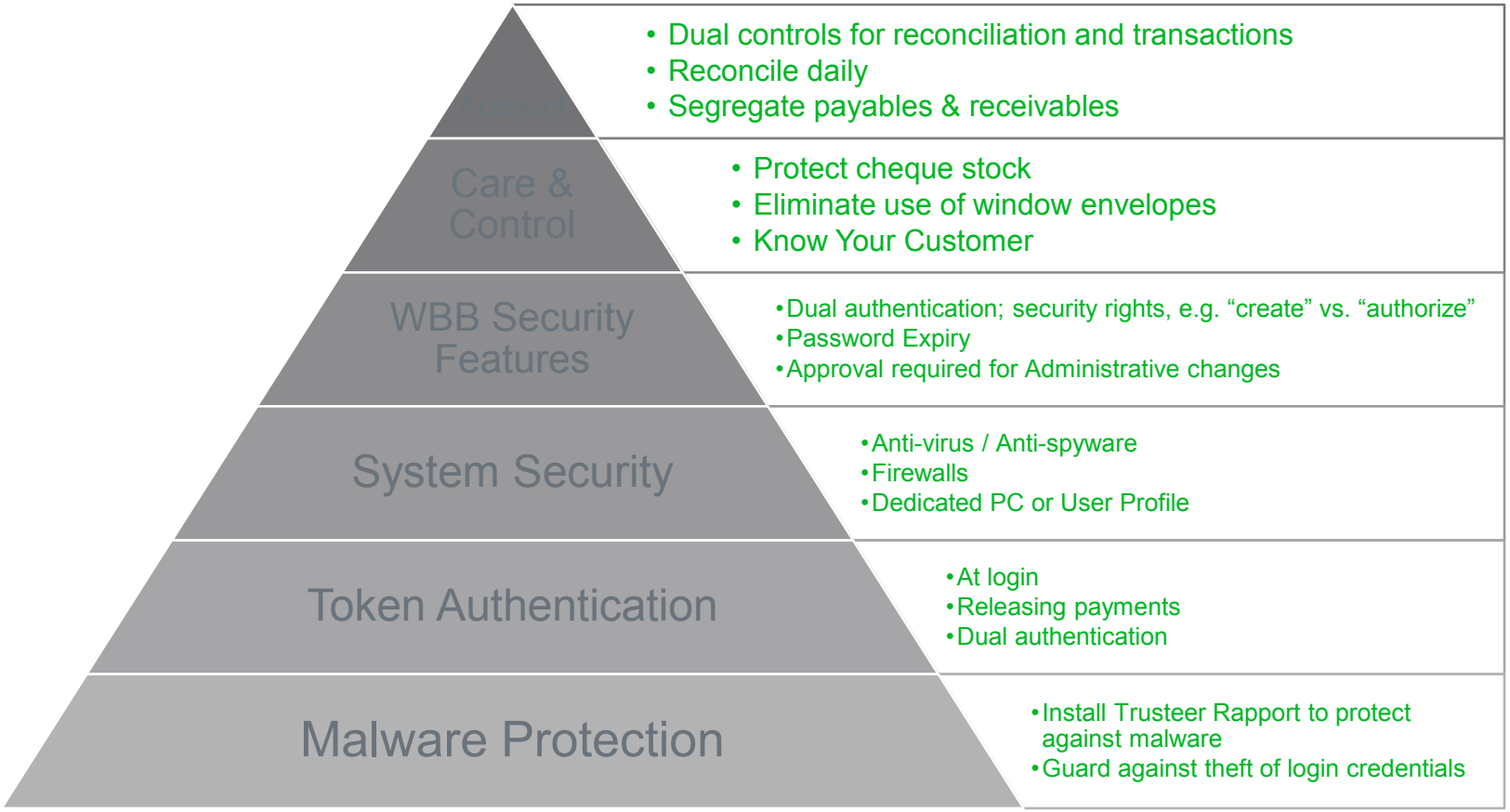
- **Prevention**
  - Always use all of the available security features within your web banking product (token authentication, dual authentication, security rights, etc.)
  - Talk to your IT professional and ensure you use up-to-date anti-virus/anti-spyware software; firewalls; malware protection; and up-to-date, supported browsers
  - Segregate duties / accounts and require **dual approval** for all payments
  - Inform your Bank immediately of any issues or concerns
- **Email is not a secure medium - treat emails with caution**
  - Confirm suppliers' instructions for account number / address changes back to them by phone (at their number on file)
  - Question payment instructions from other internal users if they seem out of the ordinary. Confirm back by phone.

Protecting Against Internal Fraud

- **Common Forms:**
  - Cash Misappropriation / Cheque Theft
  - False Invoicing
  - Expense Reimbursement Fraud
- **What you can do:**
  - Segregation of duties and / or job rotation
  - Independent reconciliation
  - Mandatory vacations
  - Automate as much of the AP process as possible to reduce risk of errors and fraud.
  - Control changes to the vendor database. Any vendors that are no longer used, and any duplicate entries, should be removed.
  - Do not allow manually generated payments that bypass the AP system and circumvent established controls.
  - Monitor expense claims closely and ask for original receipts
  - Require signoff on all expense claims

Layered Fraud Prevention Framework

- **There's no "magic bullet": layering security features is your best defense against fraud**



Thank you!

Best Practices in Fraud Prevention

24 ways to protect your company

How well-protected is your company?

No matter the type of business, the risk of fraud is always present. While you cannot predict why or when your organization may become a target, there is a lot you can do to reduce the opportunity for fraud.

We have collected some of the "Best Practices" that our existing customers have implemented to protect their financial transactions and their dealings with us. We invite you to review these tips to determine how well-protected your business is and as a source of ideas to develop a fraud prevention plan. You will see that many of these practices can be put to work easily and inexpensively. Remove the opportunity for fraud and you have gone a long way toward preventing it!

Our cash management specialists would be pleased to work with you. We can help review your needs and provide information on our products and services that are available to help your company protect itself against fraud.

Reconciliation

1. **Daily Reconciliation:** Reconcile all your business banking transactions daily. This data can be quickly and easily accessed online.
2. **Positive Pay & Payee Match:** Transmit a copy of your cheque issue file, including payee details, to us. Your daily incoming cheques can be monitored and unmatched items, including altered payee, flagged for your immediate action.
3. **Month-End Bank Statements:** Review every item on your statement, including cheque images. Let us know within 30 days if any item on your statement does not reconcile to your records.

Cheque Considerations

4. **Centralize Your Cheque Issuing:** Do not leave cheques available to unauthorized staff.
5. **Lock Up Cheques:** Securely and separately lock up unissued cheques, facsimile signature stamps and any cheque reorder forms.
6. **Enforce Security Procedures:** Maintain control of your cheque stock throughout the entire cheque printing, issuing, signing and dispatch process. Also, audit cheque stock frequently and without warning.
7. **Cheque Paper Stock:** The selection of your cheque paper stock is important. Insist on quality cheque stock to enhance your protection against fraud. Our cheque supplier, D+H™, offers many of the latest image-friendly security features such as –
   - Microprint
   - Chemical Protection
   - Fluorescent Fibers and Security Ink Message
   - Holographic Marker
   - Padlock Icon
   - Foil Stamping
8. **Magnetic Ink Character Recognition Serial Numbers (MICR):** MICR serial numbers must be used on all business account cheques clearing.
9. **Cheque Printing:** When printing and processing cheques –
   - Use a type font of 10 points or larger
   - Avoid using window envelopes

Cheque Alternatives

10. **Bill Payments:** Complete routine bill payments electronically. Internet banking services can facilitate post-dated payments.
11. **Tax Payments:** Pay GST/HST/TVQ and other complex tax payments on a Web-based tax payment and filing service.
12. **Credit Cards:** Encourage suppliers to accept credit card payments for purchases under $5,000, to eliminate small-dollar cheques. Depending on the card used, you may also accumulate rewards.
13. **Payroll Cheques:** Link your in-house computer payroll software to an Electronic Funds Transfer (EFT) Service to provide direct deposit to employee accounts. Alternatively, ask us about Ceridian®. They can handle the entire payroll and direct deposit function for you.

14. **Supplier Payments:** A payables consolidation service can be used for electronic payment to suppliers requiring backup detail of the payment being made by fax, email or Electronic Data Interchange (EDI).

15. **Bank Drafts:** Lost bank drafts can be replaced, but the original is still valid. For payments in U.S. Dollars or other currencies, consider wire transfers instead.

16. **Manual Wire Payments:** Use an online wire payment service with security features such as authentication devices and pre-authorized payment templates instead of fax or telephone instructions.

17. **Pre-Authorized Payment:** By authorizing your creditors to automatically debit your account for payments, you can manage your cash flow by knowing exactly when payments will be made.

Deposit Considerations

18. **Local Deposit Accounts:** Consider eliminating local accounts for remote offices. Direct deposits to a central deposit account and verify activity daily.

19. **Lockboxes:** Have your customers mail payments directly to a bank-operated lockbox to centralize and automate collection of receivables.

20. **Returned Items:** Use endorsement stamps that clearly direct returned items to the account of your choice.

21. **Merchant Services:** Train your employees to recognize suspicious fraud practices and establish an escalation process to report these occurrences to you. Ensure you are compliant with the Payment Card Industry Data Security Standard (PCI DSS), which protects your customers cardholder information and ultimately your brand. At all times, be sure to store sales drafts securely and maintain secure control over point-of-sale equipment, which can also be used fraudulently.

Accounting

22. **Separate the Functions:** Different people should be responsible for the writing and/or signing of cheques, and the reconciliation of the bank statement.

23. **Special Accounts:** Open separate accounts to separate such functions as incoming wires and high-volume small-dollar cheques.

24. **Security Audit:** We recommend a full audit by an accounting professional that includes a complete review of your security procedures.

Remove the opportunity for fraud and you've gone a long way toward preventing it. When you consider the financial losses, business disruption and harm to customer confidence that can come with fraud, implementing these *Best Practices* is a small price to pay. Contact your TD Commercial Banking Relationship Manager today about the many services we can provide your business to help you protect yourself against fraud.

Safe Computing

Protecting Your Computer

There are a number of things you can do that will help protect your information when you are using the Internet.

- Stay secure by using a legally licensed operating system and browser. Keep them current by downloading the latest software and security updates
- Remember to log off when you've finished your banking or if leaving your computer unattended
- Guard your usernames, passwords and login information. TD Bank Group will not ask you to provide personal information, or login information such as usernames, passwords, PINs or account numbers
- Choose unique passwords that you can remember so that you do not have to write them down. A combination of letters and numbers should be used for better protection
- Do not use passwords that are easy for others to guess such as birthdays, family names or telephone numbers
- Ensure that AutoComplete or other memorized password functions on your browser are disabled
- Saving passwords on your computer, on the Internet or on any software is not a good idea. It allows anyone with access to that information the ability to potentially impersonate you
- Never disclose your password(s) to anyone, especially online, not even to the police, your financial institution or your Internet service provider
- Protect your computer from hackers and other intrusions by installing a firewall
- Review and implement the authentication protocols available in our products and services, including segregation of duties, authorization/authentication, administration control, etc.
- Use only a stand-alone, locked down computer system for banking

- Antivirus and anti-spyware software is designed to seek out viruses and malicious programs running on your computer and remove them. Always use the most up-to-date versions
- Clear your browser's cache memory at the end of any online banking session. This will delete any pages, files and reports that your browser may have temporarily saved on your hard drive
- Email is not a secure medium of communication, similar to a cellphone conversation that can be easily monitored. You should never include banking information in an email to us or anyone else. Only general inquiries should be sent via email. Personal information that should not be sent via email includes, but is not limited to, account numbers, Connect IDs and passwords

Phishing

Phishing is a scam where a fraudster sends an authentic looking email which appears to come from a legitimate company. The intention is to "phish" (pronounced "fish") for personal and financial information. These "phishing" emails direct recipients to click on links that redirect them to fraudulent websites. These sites are designed to fool customers into believing that they are actually visiting a legitimate company website. Once on the fraudulent site, the email recipient is asked to enter personal and/ or financial information that is later used to commit fraud.

TD Bank Group will never send emails asking a customer for personal information, user IDs, passwords or PIN numbers from the authentication device.

How to Avoid Phishing Scams

While online banking is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet.

- Be suspicious of any email with urgent requests for personal financial information.
- Phishing emails typically include upsetting or exciting (but false) statements to get people to react immediately. They also typically ask for information such as Connect IDs and passwords
- Phishing emails are typically NOT personalized, but they can be. Valid messages from your bank generally are personalized, but always call to check if you are unsure
- Do not use the links in an email to get to any web page. If you suspect the message might not be authentic or you don't know the sender, call us on the telephone or log onto the website directly by typing in the web address in your browser
- Make it a habit to enter the address of any banking, shopping, auction or financial transaction website yourself and not to depend on displayed links

For more information on fraud prevention, please contact your TD Commercial Banking Relationship Manager.

To find out more about our Cash Management Services or the location of a TD Commercial Banking Centre in your area, visit www.tdcommercialbanking.com or contact your TD Commercial Banking Relationship Manager.

web_591328 (0312)