Fraud: Don't be a victim

In their 2018 Global Fraud Study, the Association of Certified Fraud Examiners (ACFE) found that organizations lose 5% of revenue each year as a result of fraud. Extrapolating this statistic to a global point of view, based on 2017 estimated Gross World Product (GWP), would result in a staggering $4 trillion dollars of loss relating to fraud.

Financial cost associated with the loss isn't the only concern for organizations in dealing with fraud. Other costs are: morale, productivity and organizational reputation. Additionally, based on the 2018 AFP Payments Fraud and Control Survey, 78% of U.S. organizations surveyed report being exposed to actual or attempted fraud in 2017—the largest percentage on record. In addition, 65% of organizations reported that checks were the primary target for fraud attacks and 54% of organizations reported being exposed to wire payments fraud via business email compromise (BEC) scams.

Although not an exhaustive list of the types of cybercrime, the following are common types of cybercrime.

Malware

Malware infiltrates computer systems and performs unauthorized activities and transactions, such as email takeover, corporate account takeover/identity theft, data breaches and theft, and denial of service.

Some ways to protect information are:

- Regularly update anti-virus and anti-malware software.
- Always verify the source of fund transfer requests.
- Ensure website is legitimate. If in doubt, type the URL into a browser to verify.
- Be aware of any changes to regularly accessed financial services websites and unusual experiences, including unusual URLs appearing in the browser window.
- Verify and validate requests to validate credentials.
- Note unusual slowness of banking session.
- Beware of requests for sign-in credentials on any page other than the sign-in page.
- Beware of emails requesting account information, account verification or banking credentials (such as usernames and passwords).

Table of contents

Continued

Phishing and spear phishing

Phishing is one of the most common ways to infect computer systems with malware. Typically, phishing comes as unsolicited emails that appear legitimate with real company names and logos, such as banks and insurance companies. The email may request personal or financial information, request that a link be clicked, or have a redirection to another website. By divulging information, malware can infect email accounts, company email addresses and corporate networks, which can lead to identity theft, corporate email takeover and facilitate hacking into databases.

Phishing is one of the most common ways to infect computer systems with malware. Typically, phishing comes as unsolicited emails that appear legitimate with real company names and logos, such as banks and insurance companies.

Other kinds of phishing

- **Spear phishing** is where criminals search social media sites, such as Facebook, Twitter and LinkedIn to identify individuals who can authorize payments. These individuals are then targeted with emails containing malware.
- **Vishing** is the same process, however, uses telephone calls.
- **Smishing** is also the same process, however, uses text messaging.

Beware of any communication requesting confidential financial information. Also:

- Be suspicious of requests by email, phone or text for confidential information regardless of real company logos or letterheads.
- Never divulge or share personal identity credentials or any financial information such as account information, usernames, passwords and PINs.
- Never divulge or share security tokens and token passwords.
- Never click on a link in a suspicious email, which may be a redirection to a fraudulent site; or by clicking, enable malware, such as spyware, to monitor keystrokes and gain access to financial information.
- Be social media savvy. Be wary of making too many professional details public on a social media site; it sets you and the organization up as targets for spear phishing.

With potential fraud becoming an increasing concern for all businesses across the globe, smaller organizations have a greater probability of being targeted as well, because they generally are under-protected when it comes to anti-fraud controls and technology security. Actions can be taken to protect smaller organizations from fraud relating to financial transactions. Where possible, seek to implement automation to processes and where automation is not possible; consider implementing Dual Control Review and Approval processes and segregation of duties. Having those able to initiate transactions separate from those able to approve transactions, in our view, lessens the probability of being the victim of fraud. Also, consider reviewing and reconciling transactions daily. Taking these steps will help identify normal patterns and allow for unusual activity to be identified more quickly.

With potential fraud becoming an increasing concern for all businesses across the globe, smaller organizations have a greater probability of being targeted as well, because they generally are under-protected when it comes to anti-fraud controls and technology security.

BMO Trust and Custody Services takes pride in knowing that together with our clients we can help mitigate fraud. The following are some steps that BMO takes in the assistance of managing fraud with and for our clients:

1. BMO works with our clients to understand the nature of their business and the associated transactions we will support. By gaining this understanding, we are in a better position to question activity that seems to be out of place. Furthermore, where possible, we seek to implement Standing Instructions that are authorized by clients, which limits the frequency of instructions from clients for standard activity, which lessens the chances that a third-party will inappropriately access the communication.

Continued

2. BMO implemented a program of standardization of client instructions for client-instructed activity and requires client signatures. These protections allow for confirmation of activity that makes sense for the work that BMO supports for our clients' organizations—and having the ability to review the signature of an authorized party adds another layer of validation to the activity.
3. BMO introduced a Secure File Transfer (SFTP) website for conveying client instructions to BMO, which keeps account information secure.
4. BMO implemented Call Back procedures for client-requested disbursements (not subject to standing instructions). By calling our clients to confirm received instruction, together we can affirm that the request was appropriate and properly instructed. Within the last six months alone, this control step stopped four instances of fraud perpetrated on our clients.
5. BMO grants access to our clients and their advisors to their authorized accounts through Portfolio Vision. This application is available 24 hours a day, 7 days a week, and is available in real time. Having access to your information gives you the power to monitor your account activity and reconcile your accounts in a timely manner.

Fraud protection starts with you and your employees. Here are a few final tips:

- Do not respond to an email requesting personal identification or financial information.
- Do not open any attachments or click on any links with which you are not familiar. The same applies to communications via telephone or text.
- Be cautious in handling websites, and verify that the site is secure by checking for the https:// designation in the browser. Look for the lock icon on the screen.
- Have tools in place for managing pop-ups and educate staff to stay away from scareware tactics or diversion to other websites requesting your information.
- Never download a program from an "unofficial" site, no matter how good the deal appears. Free programs can sometimes infect computer systems with malware.
- Do not store credit card information on websites.
- Do not use software to memorize passwords.
- Exit websites securely and clear the computer's cache.
- Keep user identifications, PINs and passwords safe at the workplace.
- Never leave the computer while sensitive information could easily be obtained.
- Be wary of making too many professional details public on social media sites; it sets you and the organization up as targets for spear phishing.

The role you and your work colleagues play in the management of fraud risks is paramount. Take time to understand the role your providers, like BMO Trust and Custody Services, play in the mitigation of fraud and how your controls can complement fraud prevention.

BMO implemented a program of standardization of client instructions for client-instructed activity and requires client signatures. These protections allow for confirmation of activity that makes sense for the work that BMO supports for our clients' organizations—and having the ability to review the signature of an authorized party adds another layer of validation to the activity.

Sources

Fraud Statistics Every Business Should Know, Quickbooks Resource Center, URL: https://quickbooks.intuit.com/r/trends-stats/fraud-statistics-every-business-should-know/#g

Report to the nations on Occupational Fraud and Abuse, 2018 Global Fraud Study, Association of Certified Fraud Examiners, 2018.

2018 Association for Financial Professionals Inc., Payments Fraud and Control Survey, Report of Survey Results, URL: afponline.org

Managing Risk: A Practical Guide to Payment Fraud. BMO Financial Group. March 2017

Let's connect

1-855-421-4993

bmotrustandcustodyservices.com

trustandcustody.services@bmo.com

bmo-global-asset-management

BMO Global Asset Management