Fraud Prevention Overview

05/14/2020

Disclaimer:

For the purposes of this overview, it should be noted that this is being provided as a courtesy. The information and materials being shared is not for providing training or advice and SMBC is not responsible for the content. This “Anti – Fraud” material is informational only.

Why Do We Care About Fraud?

In most cases, the related financial institutions absorb part of the monetary loss resulting from a fraudulent transfer. However, there are other factors to consider when you think about the cost associated with fraud.

- **Expensive remediation and investigation costs**

  It is estimated that every time you are hit with fraud, it takes 100 to 200 hours of investigation, which results in lost time and increased costs.

- **Legal Liability**

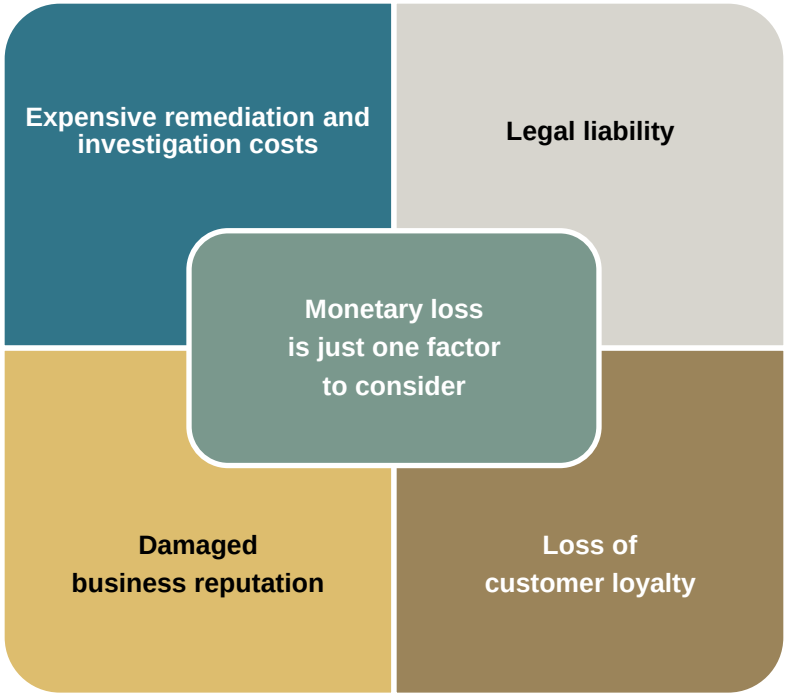
  Increasingly, victims of wire fraud have been bringing lawsuits against financial institutions because of their losses.

- **Damaged business reputation**

  Nothing will damage your reputation faster than a high profile fraud case. It is proven that 43% of business accounts will move if they have been hit with a fraud attack.

- **Loss of customer loyalty**

  Your customers will be more loyal to your institution if they know you are taking steps to protect them and their funds.



Prevalent Types of Fraud

Many types of fraud exist. This overview targets the following common types of frauds

1. **Wire Transfer Fraud**
2. **ACH Fraud**
3. **Forgery and Stolen Checks**
4. **Business Email Compromise / Phishing / Vishing and Internet Fraud**

Wire Transfer Fraud

- An increasing number of companies are falling victim to wire transfer scams, costing more than $1 billion in just the last 18 months (per the U.S. Secret Service).
- Scams are being perpetrated through fake emails from senior executives of the company or phony vendor emails.
- Public and private companies of all sizes have been affected by this type of scam. Companies with international business dealings are more likely to be targeted since transfers to overseas banks would not be out of the ordinary.
- On value date, the first three hours are critical to recall wire funds. After 24 hours, the chances are slim to none of recuperating the funds.

1) Wire fraud fraudsters use spoofed email so learn to spot it. Although there are a number of ways to spoof email, it can be as simple as this.[1] The email address of Lawfirm@aol.com is changed to Lawfirm@aoi.com or Mark.Bassingthwaighte@RECompany.net is changed to Mark.Bassingthwaite@RECompany.net.

2) Security basics are a must. Avoid the use of free web-based email. Always delete unsolicited email from unknown parties. Never open spam or any attachments contained therein. Keep your firewall, operating system and security software current. Most importantly and wherever able, use multi-factor authentication on all email and financial accounts to help prevent wire fraud.

3) Establish a policy on wire transfers and couple that with appropriate training of everyone who could be involved in a wire transfer. Mandate the gathering and verification of contact information from all parties involved at the outset of representation and prohibit the use of any other non-verified contact information during the course of representation. The most important provision of the policy would be the implementation of a process whereby all wiring instructions are confirmed by use of this previously verified contact information.

4) Everyone should be trained to be suspicious and learn how to spot wire fraud scams. Underscore the necessity of remaining vigilant at all times. Everyone should know to look for inconsistencies with email such as various email addresses in use or different spellings of a name. Requests for money to be sent to an account that is not in the name of the seller, not in the jurisdiction where the seller is, or are urgent in nature should always be questioned. Finally, remind everyone that just because the grammar and spelling looks great, that doesn't mean the email is legit. Scammers have spell check too and many of these scammers draft very well written emails.

1) Source : https://blog.alpsnet.com/the-top-5-wire-fraud-prevention-tips

Wire Fraud Red Flags

1. Customer Account Number is not included on forms. Lack of use of standard wire transfer forms.
2. The email from the customer says “I am traveling and am unable to take a call to confirm” and asks that transfer be made anyway.
3. A supplier/customer has notified by email that the payee account or name has been changed.
4. A supplier/customer has notified by email that the payee account has been changed from a corporate account to a personal account or an account in the name of an unknown corporation.
5. A remittance request has been received from an email address that is not the authorized staff member’s email address.
6. Requests for money to be sent to an account that is not in the name of the seller, not in the jurisdiction where the seller is, or are urgent in nature should always be questioned.
7. Security basics are a must. Avoid the use of free web-based email. Always delete unsolicited email from unknown parties. Never open spam or any attachments to an email. Most importantly and wherever able, use multi-factor authentication on all email and financial accounts.
8. Staff should know to look for inconsistencies with email such as various email addresses or different spellings of a name, etc.
9. Finally, remind everyone that just because the grammar and spelling looks correct, that doesn’t mean the email is legitimate. Scammers have spell check too and many of these scammers draft professional-looking emails.

ACH Fraud

The ACH system supports both credit transfers and debit transfers, which are authorized and initiated in different ways. These differences imply that fraudulent payments using ACH credit transfers and ACH debit transfers are perpetrated in different ways.

For an ACH credit transfer, the payer's depository institution initiates the funds transfer on the instruction of the payer. ACH credit transfers are typically used for routine business-to-business payments as well as business-to-consumer payments such as payroll. Third-party fraudulent ACH credit transfers would generally need to be initiated by obtaining access to or taking over the payer's account (possibly facilitated by stolen or hacked passwords or other credentials) or insider fraud facilitated by a rogue employee of a depository institution or business payer.

For an ACH debit transfer, the payee's depository institution initiates the funds transfer on the instruction of the payee who, in turn, must have authorization from the payer to initiate the payment. ACH debit transfers are typically used for consumer-to-business payments like pre-authorized automated bill payments. Corporations typically block ACH debit transfers so that fraud opportunities are mainly limited to consumer accounts. If a settled fraudulent ACH debit transfer is returned as unauthorized, the payee's bank must investigate the fraud. If the fraud determination is not communicated to the payer's bank, the fraud will not be included in the estimates.

One way ACH fraud can occur: Companies using checks may be exposed to anyone capturing their micro-encoded check information; DDA account number and the bank's ABA number. Then, the fraudster arranges for an ACH debit against the DDA account. By the time the customers reconcile their DDA account and protest the withdrawal, it may be too late to submit a claim because the fraudster has withdrawn all of the money and left the account with a zero balance; there is not any recourse.

Preventable Measures:

- When the customer's account has been compromised, it is a bank industry practice to recommend immediately closing the compromised account and opening a new account.

Sources: https://www.federalreserve.gov/newsevents/pressreleases/other20181016a.htm
https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network

Forgery and Stolen Checks

Check fraud is one of the largest challenges facing financial institutions. Technology has made it increasingly easy for criminals to create realistic counterfeit or forged checks as well as false identification that can be used to defraud financial institutions.

Fraud schemes involving checks take many forms. Checks may be:

- Altered either as to the payee or the amount
- Counterfeited
- Forged either as to signature or endorsement

Check fraud criminals may be financial institution insiders, independent operators, or organized gangs. The methods they use to further check fraud include:

- Getting customer information from financial institution insiders
- Stealing financial institution statements and checks
- Working with dishonest employees of merchants who accept payments by check
- Going through trash for information about financial institution relationships

Preventable Measures:

- When the customer's checking account has been compromised, it is a bank industry practice to recommend immediately closing the compromised account and opening a new account.
- Corporate customers should perform a daily reconciliation against their accounts. There is a two-business-day window to return checks.
- Customers should enroll in CDA /Positive Pay Services

Business Email Compromise / Phishing /Vishing and Internet Fraud

- **Business email Compromise** - A business email compromise (BEC) is an exploit in which the attacker gains access to a corporate email account and spoofs the owner's identity to defraud the company or its employees, customers or partners of money.
- **Phishing** - Phishing involves sending customers a seemingly legitimate email request for account information, often under the appearance of asking the customer to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information scams are being perpetrated through fake emails from senior executives of the company or phony vendor emails.
- **Vishing** - the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.
- **Internet fraud** - can be defined as any type of scheme that uses one or more components of the internet (e.g., chat, email, website) to publish fraudulent solicitations, conduct fraudulent transactions, or transmit proceeds obtained through fraud.

Preventative Steps			
Business Email Compromise	**Phishing**	**Vishing**	**Internet Fraud**
• Enable multi-factor authentication for business email accounts. Multi Factor Authentication can consist of various types of authentication including information to log in, such as a password and a dynamic pin, code, or biometrics • Beware of opening any email for unknown senders. If you open an email from a unknown sender do not open any attachments or links. This can allow for malware to access your computer system computer system • Know the behavior of your customers and vendors. Identifying changes in business practice can prevent potential fraudulent activity	• Remind customer that the bank will never request confidential information through email and they should report any such requests to the bank. • Verify the identity of the Correspondent, verifying the Identify of the user can protect the user from Fraudulent emails and other fraud	• Be apprehensive of unknown callers. Do not provide information to the caller unless you can verify the identity of the caller • If the caller is attempting to solicit information from you, tell them you will call them back but first verify the legitimacy of the company. Never provide information or other private information to anyone an unknown caller .	• Do not give out any information regarding your savings, checking, credit, social security number or other financial accounts • Deal only with legitimate, reputable companies and individuals. • Work with your internal and/or outsourced IT teams to secure your Fire-wall, Network and Infrastructure environment. • Enhance your Onboarding (in-depth background checks) process specific to IT hires.

Fraud Prevention Best Practices

1. The best defense against phishing scams is to assume the email is untrustworthy and to pursue direct channels to businesses that you trust! Adhering to the established policy confirming the wire transfer via telephone with the “List of Authorized Personnel” (Authority and Indemnity in Respect of Telephone, Facsimile, E-mail, and Mail Instructions) is your best option. Any potential fraud case should be escalated to your manager and your Fraud Team.

2. When replying to a customer email request, we strongly recommend using the “forward” function instead of “reply” and typing in the correct email address obtained from an official document (*e.g.*, business card), as well as using a password-protected attachments for increased security instead of including information on payment or remittance instructions in the body of the email.

3. Ensure that all staff are properly trained to be suspicious and learn how to spot wire fraud scams. Staff should know to look for inconsistencies with email such as various email addresses or a different spellings of a name, incorrect forms or wording that do not comply with our standard Policies & Procedures. Underscore the necessity of remaining vigilant at all times.

4. When confirming with your customer a remittance instruction change, encourage your customer to confirm via phone to their authorized counter party personnel before any funds are remitted -- especially when the request is unusual and deviates from normal billing.