ABA Insurance Services

MEMBER OF GREAT AMERICAN INSURANCE GROUP

10 best practices to implement now to

AVOID WIRE FRAUD AT YOUR BANK

Wire Fraud involving bank customers is exploding! The 2017 ABA Deposit Account Fraud Survey Report* found that bank deposit accounts are the targets of over $1 billion in wire fraud attacks annually. It is insufficient to rely upon insurance to make you and your customers whole as insurance will not cover 100% of wire fraud incidents or 100% of every wire fraud loss. Further, insurance carriers expect banks to exercise a minimum level of due care to prevent any crime, including wire fraud crime. Frontline personnel are in the best position to both spot and prevent wire fraud; therefore, it is critical that banks undertake these best practices.

1. Train employees to identify phishing emails

Phishing scams are the initiation point to many wire fraud crimes involving the bank's money. In a phishing scam, an employee opens an email containing malware that allows the fraudster to infiltrate the employee's computer. This access results in a fraudulent wire transfer request via a social engineering scheme. For example:

- *A senior executive's email account is taken over through malware installed by a successful phishing attack, allowing the fraudster to initiate a seemingly internal request to wire bank funds to a fake vendor.*
- *A loan officer responsible for approving HELOC transfers was phished. The perpetrator used his access to the loan officer's computer to create both fraudulent customer transfer requests and bank approvals based on accurate banking information found in the employee's email history.*

To reinforce the training, test your employees' ability to identify phishing scams through simulated attacks. This will help them—and your bank—avoid becoming a phishing victim.

2. Train customers to understand the threat caused by phishing attacks

Phishing scams are the initiation point to many wire fraud schemes involving your customer's money as well. Avoid a potential conflict with your customers and seek to educate them on threats to their hard-earned money from phishing attempts and other cyber crimes.

3. Ensure that you have written agreements with all customers prior to wiring funds

A written agreement is a document that outlines your customer's preferences regarding the transfer of funds from a particular account. You should have a written agreement in place prior to the first wire transfer request in order to avoid any confusion about their wishes. The agreement should:

- Include the customer's explicit authorization for the bank to execute wires, and the means by which wire transfer requests may be requested (e.g., via email, telephone, or in person);
- Contain the names of all individuals granted authority by the customer to initiate such requests; and
- Outline a commercially reasonable security procedure that will be utilized by the bank and the customer to authenticate all requests.

Please note that a wire request–a form completed by the customer to initiate a specific wire transfer–is not the same as a written agreement. The absence of a written agreement will likely result in a claim denial with many insurance carriers.

4. Perform a callback on wires to a predetermined number to authenticate wire requests

While some insurance policies allow variations in authentication procedures, a phone call to the customer's number on file is still one of the best ways to prevent fraud. It is much easier for a fraudster to take over email addresses than phone numbers; however, this method is not foolproof, so be sure to review the account for any phone number or named individual changes within the past year. Legitimate changes to established wiring authorization instructions are rare–assume fraud if recent account changes on file have been made and seek independent verification.

5. Perform an out of band verification to authenticate wire requests

When a callback is not practical or preferred by the customer, use an out-of-band verification to authenticate wire requests. *The type of verification method should be established in the written agreement.* Do not sacrifice sound authentication procedures for customer convenience. "Electronic money" is still money and the same level of care should be taken with electronic funds as vault cash. Also, as noted above, legitimate changes to established wiring authorization instructions are rare, and the receipt of a request for procedural changes should be a red flag requiring additional verifications.

Continued ⇨

10 BEST PRACTICES TO IMPLEMENT TO AVOID WIRE FRAUD AT YOUR BANK *continued*

6. Require extra scrutiny of international wires

Ensure your wire procedures require extra scrutiny for requests to transfer money overseas. These transfers are particularly problematic as they are often difficult to recall if they are found to be fraudulent. Train employees to assume that international wires are fraudulent until proven otherwise, especially if the transfer amount is in excess of an established dollar threshold.

7. Require extra scrutiny of wires tied to HELOC accounts

Due to the public nature of HELOC information, criminals can easily impersonate bank customers and request fraudulent transfers out of HELOC accounts. The importance of having a written agreement establishing permission for wire transfers and commercially reasonable authentication procedures is especially critical for HELOCs.

8. Require extra scrutiny of wires tied to real estate transactions

Real estate wire fraud often involves a type of social engineering where criminals impersonate the title or real estate agent handling the property sale. The agent's email is either forged or hacked and used to send an email to the property buyer who in turn provides wire instructions to a fraudulent bank account. Be mindful that there may not be insurance coverage for the bank under this scenario because the bank is properly following their customer's directions and therefore, has no legal liability for the loss.

9. Do not immediately refund lost funds to the customer

If fraudulent wire activity is discovered, do not automatically refund the stolen customer funds. While business decisions to immediately restore the customer to whole are good for the relationship, such business decisions are not insurable and could cause the denial of coverage under the insurance policy. Instead, contact your insurance carrier to report the fraud first and work with the carrier to lay out the best course of action. Be aware that coverage under a liability policy requires:

- A written demand from the customer requesting the restoration of funds or alleging a wrongful act;
- Legal liability on the bank's part; and
- The insurers consent before any settlement with the customer can be made.

10. Immediately attempt to recall lost funds from the corresponding financial institution

Timeliness is key here. If bank personnel let a fraudulent wire instruction slip through, but quickly discovered it on the back end, the bank may be able to recall the funds from the receiving financial institution. Your bank has a better chance of succeeding if you have a policy that details these steps and if your personnel is trained to act rapidly.

Wire Fraud continues to be a challenge for all banks. Ensure that your bank is following best practices to mitigate the exposure and risk of wire fraud losses.

*Source: 2017 ABA Deposit Account Fraud Survey, published January 2018, American Bankers Association, www.aba.com