Managing Wire Transfer Fraud Risk

Know your customer. Likely most everyone in banking has repeated this mantra time and time again. In today's digital age of banking, it may seem impossible to truly know the customer, but it's becoming as important as ever. Wire transfer fraud is an increasing trend in financial institutions and may continue to grow in the coming years. When hundreds of thousands of dollars can be transferred with just the click of the button, knowing your customer can help banks to be on the lookout for signs that may alert the institution to a potential fraud attempt.

Today's "bank robbers" know it's far easier to rob someone with a computer or a telephone than with a gun – and it's safer, too. Electronic theft began in the early '80s as banks began implementing computer systems to track customer accounts. Criminals quickly learned that getting into a customer's electronic account is much easier to access "through the front door," using a customer's personal information. The same principle holds true today. Wire fraud can occur through the phone, fax, email or online, and the losses average hundreds of thousands of dollars per incident. That's a lot of money moving around, often without ever hearing the person's voice. Criminals have countless methods for convincing a bank to wire large sums of money to another account, but the results tend to be similar:

- a fax to a bank with a customer's information that the customer did not send
- a memo from a call with the "customer" which the customer never made
- an email from the customer's account that the customer did not write
- a confirmation phone call to the number listed in the account, only to later find the number has been temporarily diverted by the criminal, meaning the verbal confirmation comes from the thief, not the customer

The victims can be individuals, but businesses are more likely to fall prey to these schemes since they tend to carry heftier account balances than individuals. Small businesses are targeted the most frequently. They generally lack the complex security measures of larger organizations and criminals find it much easier to access sensitive information.

The majority of fraudulent foreign wire transfers wind up in Asia, Eastern Europe or Africa. These international transfers are the most dangerous because there is no government protection and no way to reverse the process. Domestic fraud isn't uncommon either. In the United States, wire transfers have some safeguards in place to manage fraud, but it should be assumed that once a transfer is made, there is no way to bring the money back. The responsibility for the stolen money could fall on the account holder and/or the bank depending on the circumstances.

Help Safeguard Against Fraud

There are endless ways criminals will find to transfer someone else's money into their own bank accounts, but there are a few red flags that should help alert the teller executing the transfer that something may be amiss. Some situations to keep an eye out for are abnormally large transfers, transfers from an account that has never wired money in the past and any transfer to Europe, Africa or Asia. Another warning sign is someone who has excuses as to why he or she can't speak with you over the phone. Banks can help protect themselves and their customers by paying attention to these and other red flags and by putting safeguards in place to help spot potential wire transfer thefts before they happen.

Consider Executing Account Usage Agreements

Usage agreements can detail things like who is authorized to execute a transaction, which accounts are eligible for transfers, what security measures and verification steps are in place, which communications methods are used and who is liable for what if fraud were to occur. These agreements can be especially

useful for businesses, but should be considered for individuals as well. Another step to consider could be to require individual, international or first-time transfers to happen in person, or implement digital security tokens that generate a new unique user password every few minutes. Phone passwords can also help distinguish the true account holder from a criminal.

Think About Creating Transfer Procedures

Many times fraud occurs because the protection process broke down somewhere along the way. As a result, banks should consider having a formal process for transferring funds and training employees to follow all steps in the process. For example, if the process requires a teller to call the number listed in the account after a transfer is initiated, then a teller should place the phone call. Often criminals will call immediately after faxing a transfer request to "make sure the fax went through." Speaking to the person executing the transfer should not replace calling the number listed in the account.

Know Your Customer

As mentioned before, knowing the customer is as important as ever. Does this customer normally transfer money? How big are the transfers? Where does the money usually end up, somewhere local or an international account? In what ways do they typically initiate a transaction and who is the originator? Is the origination account the one that is normally used for transfers? If speaking to someone on the phone, do they sound to be the same gender as the name on the account? Knowing the answers to these questions could help alert bank employees to potential fraud in progress.

Consider Training Employees Who Conduct Transactions

Bank employees should trust their instincts when something seems amiss in a transfer request. Consider teaching these employees the warning signs that could help alert them to potential fraud – even if it might be to the temporary annoyance of the customer. While keeping customers satisfied and ensuring quick transactions are important, secure banking is the paramount concern. Ultimately, customers will appreciate your efforts toward the security of their money more than they will a quick, easy transfer. Encourage employees to trust their judgement and follow the security procedures, which may include review with the bank's security officer.

Encourage Customers and Employees to Protect Sensitive Data

It's incredibly important to protect sensitive data such as social security numbers, account numbers and passwords. In today's society, it's unnerving how easy it is to build a complete personal profile of someone using social networks and internet searches. Consider keeping digital information safe by using protected wireless networks, security software and creating strong passwords with letters, numbers and symbols. A hacker who gets into a company email system will have access to email records that may have past transfer information, giving the hacker a "template" for how to conduct the fraudulent transfer. According to a recent alert from the FBI, hackers are even initiating transactions using variations of legitimate email addresses– such as changing a letter "O" to a zero. Consider establishing protocols for safe email practices that include avoiding sending account information via email.

About OneBeacon Financial Services

OneBeacon Financial Services offers property and casualty coverages for commercial banks, savings banks and savings and loan institutions, security broker-dealers, investment advisors, insurance companies and credit unions. Specialty coverage, including management liability, professional liability, cyber liability and financial institution bond, are additionally available for institutions with less than $3 billion in assets.

Contact Us

To learn more about how OneBeacon Financial Services can help you manage your unique risks, please contact Craig Collins, President, at ccollins@onebeacon.com or 952.852.2434.

Learn more about OneBeacon Financial Services at onebeaconfs.com.