intact INSURANCE financial services

NEWS FROM THE VAULT

June 2020 | Issue 23

Keeping Customers Safe in a Remote Environment- Wire Fraud

BY CRAIG COLLINS- PRESIDENT, FINANCIAL SERVICES

These days more people are working remotely than ever before and many tasks previously done in person are happening online - including banking. Unfortunately, fraudsters are aggressively taking advantage of potential vulnerabilities that arise from this increased online activity.

Businesses are acclimating to the current unusual circumstances by offering additional services virtually. For community banks, this means working with customers by email or online, allowing electronic signatures on important documents, among other virtual services, which opens up the door for an exposed environment. Should these cyber criminals gain access to Personally Identifiable Information (PII), they can easily pose as the bank “customer”, another financial institution, another party to the transaction, or even someone else within the bank looking to transfer funds.

While wire transfer fraud is certainly not a new source of loss for community banks, criminals have been exploiting the increase in electronic and remote banking. They are constantly finding different ways to perpetrate this type of fraud. Therefore, it’s extremely important to stay vigilant while customers and employees are remote.

Security Alert – Wire Transfer Fraud involving Real Estate Loan Proceeds

There has been a significant uptick in wire transfer fraud schemes involving real estate loan proceeds and wire transfer instructions purportedly from a title attorney/agent or someone else in the bank. The transfer requests and wire transfer instructions are coming in via phone, fax and

email. Whenever requests and instructions are received via phone, fax or email – whether from a customer, another financial institution, a title attorney, a real estate agent, or even someone else in the bank – consider having employees follow the same out-of-band verification procedures that would be performed on any other wire request. Not just with the initial request and instructions, but also with any change in the request of instructions (i.e., when new receiving bank account information is received).

There has been a significant uptick in wire transfer fraud schemes involving real estate loan proceeds and wire transfer instructions purportedly from

This could start by reviewing the requestor's account and confirm that the bank has a written agreement with the customer authorizing the bank to transfer funds on deposit in reliance on instructions received via phone, fax or email. Other considerations may include:

- Is it unusual for this customer to request a wire transfer?
- Has there been a recent transfer of funds into the account from a home equity line of credit? Fraudsters frequently target home equity lines of credit since customers are not as vigilant in checking the status of these accounts. Additionally, information on the existence of these accounts is publicly accessible.
- Are the funds being transferred to a foreign account?
- Does the customer seem to be in a great hurry to complete the transfer?
- Is the request coming from a legitimate email address? Fraudsters often use email addresses that are very similar to a customer's legitimate email address (i.e., using the number "1" in place of the lower case letter "l"). Review email addresses closely.
- Has the phone number on file for this customer recently been changed?
- Has the receiving bank account information, or any other material detail of the request, recently been changed?

Additional steps to help mitigate risk could include:

- Updating customer files with alternate phone numbers so that callbacks can be made to multiple phone lines.
- Using a multi-factor authentication method. Work with your customer in advance to record at least three different security questions and answers that only they would know the answer to. When performing a callback during a transfer request, ask the customer each question.
- Establishing alternate electronic verification methods, such as PIN numbers or security tokens.
- Executing a written agreement that details who is authorized to execute a transaction, which accounts are eligible for transfers, what security measures and verification steps are in place, which communication methods are used and who is liable (and for what) if fraud were to occur.
- Elevating all out-of-the ordinary requests, and encouraging employees to view every wire transfer request with a healthy dose of skepticism.

While it is understandable that the bank would like to make the transfer process as easy as possible for its customers and others involved, it is important for the bank to recognize the risks and take the necessary steps – before and after receiving the request – to protect its customer's money and its own money. Customers and others involved should understand that such measures are to their benefit, and they should appreciate the relatively minor inconveniences associated with verifying the legitimacy of the requests. With wire transfer fraud schemes becoming more frequent and complex, it is more important than ever for banks to protect themselves against this formidable risk.

vary by state; exclusions and deductibles may apply. Please refer to your insurance policy or consult with your independent insurance advisor for information about coverages, terms and conditions.