HOW CYBER STRONG ARE YOUR WIRE TRANSACTIONS?

According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), cyber crimes involving wire transactions are rising exponentially, exposing borrowers and our industry to catastrophic losses. The Federal Trade Commission, Financial Crimes Enforcement Network (FinCEN), National Association of Insurance Commissioners and state and local officials have all issued similar warnings in recent years as these scams have become more prevalent and sophisticated.

Title and settlement service providers can protect themselves by increasing staff awareness of these scams — and because cyber criminals are continually honing their techniques to stay a few steps ahead of unsuspecting victims, constant education and training are vital to thwarting these growing threats. Here are five of the most common red flags seen in cyber crimes involving wire transactions, and some easy ways to deflect them.

NATIC®
NORTH AMERICAN TITLE INSURANCE COMPANY

SIMPLE. DONE RIGHT.

1 HACKED EMAILS

Cyber criminals are increasingly impersonating home sellers and buyers, real estate agents and brokers, title companies and lenders, usually via email. They often monitor email exchanges between the parties of a real estate transaction to gain specific information such as names, property addresses and associated file numbers. As the scheduled closing date approaches, the scammer sends out a last-minute email from a hijacked account seeking to revise or change the wire instructions — and divert the funds elsewhere.

Plan of attack: Wire instructions rarely change at the last minute; you should always discuss the closing process and money transfer protocols with your settlement or real estate agent so everyone is clear on what to expect. Call the parties to verify that the email is legitimate using the phone number they provided you; do not use any alternate phone numbers that may be in the email. Do not respond to the email or click on any links it may contain, as they may introduce malware that can weaken your company's IT and security systems. And be sure to let all of the involved parties know that their transaction has been compromised and is being monitored so they can address any breaches and secure their accounts.

2 EMAIL IMPOSTER

Another common email scam involves the fraudster posing as a party to the transaction via email and requesting changes to the planned wire transfer — but upon closer inspection, you notice that something about the email is a little "off." For example, your seller's legitimate email address may be john-doe@abctitle.com, but this email has been sent from john_doe@abctitle.com. That's a subtle — but crucial — difference. These email scammers also often use poor grammar or spelling mistakes, which should immediately raise concerns.

Plan of attack: Develop an eagle eye for these scams. Carefully examine all email addresses and verify that they match those in your file. But most importantly, never email financial information, as email is not a secure way to handle your customers' sensitive, nonpublic personal information. Always call the involved parties using the phone numbers you collected during the closing process to verify any email requests.

3 LAST-MINUTE TRANSACTION CHANGES

When it comes time to transfer funds, you notice some discrepancies between the account number and the number you have on file. The name of the authorized person on the account may also change to someone who has not previously sent wire instructions, with this new individual claiming that the true party is on vacation, out of the country on business,

attending to a family emergency, etc.

Plan of attack: Call the involved parties and the bank to verify contact and account information. Your bank may also be able to compare the receiving account number to account numbers identified in past consumer complaints as the destination of other fraudulent transactions. Alert all of the parties and law enforcement authorities if you receive instructions containing alternate account information.

4 FOREIGN ACCOUNTS

Emailed transaction instructions direct wire transfers to a foreign bank account.

Plan of attack: This should raise an immediate red flag, and once funds find their way to a foreign account, they usually cannot be recovered. Always confirm the transaction details by calling a known and verified phone number, and refrain from handling wire transactions via email.

5 NEW DEAL OUT OF NOWHERE

You may suddenly be contacted with a new contract, associated check for earnest money or a request to immediately return all or a portion of the wired funds. These scammers gain an advantage by pressuring you to take action quickly to satisfy your customers, leaving you with little time to independently confirm all the facts.

Plan of attack: Be leery of new or unfamiliar customers or business sources, and any demands to close immediately. Slow down and take the time to call the involved parties to discuss any deviations from the transaction you agreed to handle.

Although these red flags do not necessarily mean a transaction is fraudulent, they do mean that you need to take extra steps to ensure that the alternate requests or the transaction itself is legitimate. You may even notice the presence of a few of these red flags; the more red flags you spot in a transaction, the more caution is warranted. Be sure to discuss any of these warning signs with your staff, title officer, manager, supervisor or NATIC underwriting counsel.

This report is part of our 2018 Cyber Strong campaign. You will continue to receive news and tips from NATIC on how to fight the growing incidence of cyberfraud. ***Next up: It can happen to you; Cyber fraud impacts us all.***

NATIC®
NORTH AMERICAN TITLE INSURANCE COMPANY

SIMPLE. DONE RIGHT.

www.natic.com