A NEW WRINKLE ON WIRE FRAUD
COUNTERFEIT MORTGAGE PAYOFFS

March 27, 2019
By: Matthew J. Lynch
Underwriting Counsel for Title Resources Guaranty Company

Fraudsters are attacking real estate transactions and title companies in new ways every day. In addition to the fraudsters attacking our buyers by providing fake wire instructions, or attacking our seller's proceeds by calling the title company after closing and requesting that a wire be sent in place of the check delivered at settlement, the latest scheme is an attack on mortgage payoffs.

The source of the crime is same as previous crimes; the fraudsters use social engineering, spear phishing and malware to gain access to our emails, fax systems and computers. Internet portals are also being spoofed, which means the fake portal will mirror the true website, but is the fraudster's website.

EXAMPLE OF A PAYOFF WIRE FRAUD SCHEME

When a payoff is requested, the title company receives an email that appears to be a legitimate communication from the financial institution redirecting the title company via a link in the email to the spoofed site where account and other non-public personal information is entered. The fraudster then provides the title company with an altered or outright counterfeit payoff statement with wire instructions directly to the account of the fraudster. The title company following the instructions on the fraudulent payoff statement, then wires the funds directly to the bad guys. Typically, those funds are then re-directed out of the country almost immediately.

It does not matter how the payoff is received via fax or email, examine every payoff statement very closely. If there is a SWIFT-BIC code, it means that the initial domestic bank that the funds are being transferred to will then send the funds to an international account. After the funds are out of the country there is little the FBI can do to recover the money. A SWIFT-BIC code is a huge RED FLAG.

TIPS ON PREVENTING MORTGAGE PAYOFF FRAUD

- Independently verify all wire instructions before sending. Call the institution by using a phone number that was not in the email or payoff statement. Look it up yourself.
- Examine all payoff statements received. If you have received an updated payoff with altered or modified wire instructions, stop and verify which payoff is real. Call the institution to verify the real instructions by looking up the number. The number on the fraudulent statement will be to the fraudster. Fraudsters are hoping that your guard will be down and that you will just wire the funds as directed without question.
- Compare the wire instructions with the wire instructions you may already have in your software system, i.e. for national lending institutions such as BB&T, or Bank of America, Chase, you probably already have their information and can compare the wire instructions on your payoff to those in your system. If the instructions are different, stop and verify.
- Pay attention to all the details on the statement. A payoff for a BB&T loan should not be going to Chase. Is the account name on the wire instructions the same as the payee that should be receiving the payoff? NOTE: Banks ultimately will be guided by the account number rather than the exact name on the account. When instructing the bank to wire to a certain account number, the bank will not be liable if they followed your instruction.

- Is there a SWIFT-BIC code on the wire instruction? STOP - this is an indication that the money is being redirected internationally. Once the money is outside of the US, the FBI is may not be able to recover the funds.
- Cyber- crime policies may not provide coverage, if the insured is at fault, i.e. initiated the transfer. Make sure your policy has coverage for social engineering related crimes, business email compromise fraud, wire fraud.
- If you are or suspect you are the victim of wire fraud:
    - (i) contact your bank immediately to see if they can recall the funds;
    - (ii) contact the FBI by reporting the crime to the IC3 unit at www.IC3.gov and/or www.complaint.IC3.gov (that's an "i" as in investigation);
    - (iii) the FBI has a program called the Financial Fraud Kill Chain (FFKC) that can be used to recover substantial international wire transfers that have been stolen through email scams and other crimes. The FFKC can be used if the fraudulent wire transfer meets all the following:
        - the transfer is $50,000 or more;
        - the transfer is international;
        - a SWIFT recall notice was initiated;
        - the FBI is informed of the details within 72 hours;
    - (iv) alert everyone involved to the possible fraudulent activity surrounding the transaction; and
    - (v) if your account is attacked immediately change all user names and passwords.
- Passwords should be compliant with ALTA Best Practices and be complicated, changed frequently and not shared amongst accounts, users or services.
- Use 2 factor authentication (2FA) processes on email accounts. Your account cannot be accessed without the 2nd authentication even if the password is compromised.
- Do not use free email services such as google, yahoo or similar providers.
- Do not assume a fax is any safer than an email. If you do fax, make sure to use a secured fax service in which the data is encrypted. Monitor the fax account to ensure that the fax is only being forwarded to the proper designated email accounts.
- Do not conduct business over a public wi-fi network without using a VPN (virtual private network).
- Whenever possible overnight the payoff to the verified address of the financial institution, rather than using a wire.
- Educate buyers, sellers, agents and your staff on the potential hazards of wire fraud and how to identify the risks.
- Review your policies and procedures to make sure you have and are following the latest safeguards.

Finally, please remember to always be on guard. As humans we are our own weakest link and the bad guys know that.