The Rise of Wire Fraud: Cybercrimes Targeting Money Wired in Real Estate Transactions Increasing

10/02/2018

No one can argue that technology has worked wonders in the area of real estate transactions, making these transactions faster, smoother and more accessible. However, thanks to technology these transactions are now exposed to an increased threat from criminals working in digital spaces. Perceived as an easy target various reasons, including the fast pace of transactions, the value of information and quantity of money exchanged, and the distribution and mobility of the parties involved in a transaction, businesses that engage in real estate transactions, commercial and residential, cannot be too careful when utilizing technology to modernize transaction processes.

In intercepting real estate transactions, cybercriminals are usually looking to obtain one of two items: information or money (or both). Real estate transactions include valuable information on individuals: financials, credit reports, various agreements and applications. The information being sought, such as name, dates of birth, addresses, social security numbers, bank account information, email addresses, could be made available to a cybercriminal just as easily from a real estate business as it would from a national retailer or healthcare entity, if not more so.

The simplest forms of financial phishing typically try to obtain personal financial data, such as usernames and passwords, or network access, to use, sell or share for ulterior motives. While real estate transactions are vulnerable to theft of both information and money, this article will focus on those attacks that result directly in wire fraud.

Indeed, the last two years have seen a significant increase in cybercrimes targeting money wired in connection with real estate transactions. Cybercriminals are aware the parties involved with real estate transactions typical hold and exchange large amounts of money. Historically, cybersecurity attacks have targeted larger companies, but attacks on smaller businesses are on the rise because these businesses often do not have the resources to prevent or respond to the attacks. Just last month the FBI issued a public service announcement stating cybercriminals have “heavily targeted” the real estate sector for business email compromise scams.[1] The FBI reported in this PSA that May 2018 saw the highest number of business email compromise scams for real estate victims since 2015.[2]

As example of how these attacks play out, a title officer may receive a phishing email that looks legitimate and leads the title officer to unwittingly allow a cybercriminal to access to the title officer’s system. Because the cybercriminal can monitor the behaviors of the title officer, the cybercriminal will be able to determine an opportune time to send a fraudulent email to a buyer or lender to wire funds to the cybercriminal’s bank account. There may also be a sense of urgency in the wire request. The cybercriminal’s email and instructions may appear legitimate: the email may include the title company’s

logo, the correct title company information, correct information regarding the parties to the transaction or even the correct email address of the title officer. Ultimately, this email directs a buyer or lender to wire funds to an account setup and controlled by the cybercriminal. Upon transfer, the cybercriminal immediately withdraws the funds from their account, making it too late for a buyer or lender to recover the funds upon the discovery of fraud. Historically, these attacks have been directed on buyers rather than sellers, but anyone who has the ability to send or receive funds by wire transfer from the title company to a bank may be a potential target.

Though banks are not usually a target, they are still at risk when providing loans for collateral-based lending because funds are typically routed through a third party, such as a title company. When those exchange channels are intercepted, lending institutions also incur a direct loss. As a result, multiple practices are available to further protect an institution's information and funds:

- Use Secure Computer Systems and Email Accounts. Parties to real estate transactions should avoid free web-based emails systems and free security from browsers. Secure systems and accounts can filter and block contaminated emails, virus and other attacks to keep a business transaction secure. Multi-factor authentication to log in to email systems may also provide heightened protection. Sensitive information should never be transmitted from a public IP address.
- Communicate Best Security Practices to Employees and Clients. An institution should communicate clearly and often to the individuals in its network regarding good security practices. Passwords should be changed on a regular basis and contain a strong and distinctive phrase. Personal financial information should only be sent via encrypted email. Emails, links or attachments from unidentified users should not be opened. A user can pause or hover his or her mouse over a sender's address to reveal any address discrepancies between the name of the sender and the actual email address from which the communication came.
- Pay Attention to Payment Requests. Institutions should take time to verify change requests. Cybercriminals often use a sense of urgency to instigate a wire transaction, so an organization should be guarded of time constraints identified in a request. Be aware of the need for secrecy or sudden changes in business practices, such as a change in email address. Similarly, any request sent via email to change payment accounts should be reviewed for signs of suspicious activity. If necessary, delay payment in connection with a request to change payment accounts.
- Verify and Authenticate Payment Requests. It is best to furnish clear payment information to relevant parties involved in a real estate transaction, but this is not foolproof. An institution may require multi-factor authentication in sending or receiving payment information or a change to payment information. This authentication system may be sending an email to confirm the payment information; provided these emails are not sent using the reply feature in email. The FBI cautions individuals to "be wary of any communication that is exclusively email based" and recommends establishing a secondary means of communication.[3] It may be a prudent practice to confirm all emailed wiring instructions directly with the title agent or escrow officer verbally, repeating the correct account number information on the telephone before taking any steps to transfer funds. However, the FBI also advises to be mindful of phone conversations, as reports of scams have included requests of personal information for verification purposes, and even suggests establishing code phrases only known to the two legitimate parties.[4]

As wire fraud continues to rise, lending institutions must be vigilant in verifying digital identity of parties receiving funds in real estate transactions.

Republished by permission. This article was written for and appeared in the August issue of The Arkansas Banker, page 24 and 25.

---

[1] https://www.ic3.gov/media/2018/180712.aspx

[2] https://www.ic3.gov/media/2018/180712.aspx

[3] https://www.ic3.gov/media/2018/180712.aspx

[4] https://www.ic3.gov/media/2018/180712.aspx

This article was originally published in the August 2018 issue of *Arkansas Bankers* magazine.