



## Continued Rise in Business Email Compromise – Real Estate

The United States Secret Service continues to see a sharp rise in Business Email Compromise (BEC) incidents – both successful attacks and thwarted attempts - across all sectors of business and industry. From 2019 to present, the U.S. Secret Service has seen the frequency of reported BEC incidents increase. Particularly, due to several underlying factors, the Real Estate industry has been hit hard in several different ways.

- 1) Buyer payments are being intercepted through stolen confidential and contemporaneous information, then fraudsters are using a spoofed domain to send fraudulent wiring instructions to the home buyer.
- 2) Mortgage/loan payoff payments are being intercepted through fraudulent wire instructions being inserted into the transaction process and changes in payment information are not being confirmed and/or scrutinized by the parties involved.

The first real estate BEC scenario is particularly egregious because it affects individual home buyers, often first-time home buyers, where a significant portion of life savings and personal wealth is at risk. Also, the home buying process is unfamiliar and complex to the standard home buyer, which leaves them vulnerable to BEC schemes as red flags are not detected and seen as normal due to the unfamiliarity with the home buying process.

The second BEC real estate scenario carries higher risk because the amounts of the mortgage and loan payoffs are significantly higher. For instance, the Global Investigative Operations Center (GIOC) recently intercepted a commercial loan payoff in upwards of \$21 Million that fell victim to a BEC scheme. Through swift intervention, the GIOC was able to interdict the transaction and ensure the funds were returned to the victim. There are several vulnerabilities that allow these schemes to succeed. The volume of these transactions has increased with the rise in real estate transaction activity, therefore responsible parties are processing these transactions more quickly and not seeing red flags and warning signs. Also, due to the increased transaction volume, parties involved are not confirming payment instructions before processing the transaction.

There are numerous ways to prevent real estate Business Email Compromise schemes:

- ✓ Update procedures to ensure proper verification of information before releasing funds.
- ✓ Independently obtain mortgage payoff statements and confirm with verified and trusted sources.
- ✓ Independently verify the authenticity of information included in correspondence and statement.
- ✓ Enable Multi-Factor Authentication (MFA) on all email accounts.
- ✓ Routinely change passwords.
- ✓ Routinely monitor email account access, check for unauthorized email rules and forwarding settings.
- ✓ Restrict wire transfers to known and previously verified accounts.
- ✓ Pay using checks when the information cannot be independently verified.
- ✓ Have a clear and detailed Incident Response Plan. For more information visit the Secret Service [Preparing for a Cyber Incident page](#).

***If you experience a Business Email Compromise Incident, contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF).***

<https://www.secretservice.gov/contact/field-offices/>

