WHITEPAPER:

BEC FRAUD PREVENTION IN THE REAL ESTATE INDUSTRY

TIMIOS

TITLE & ESCROW SERVICES

CONTENTS

ABSTRACT

This whitepaper reviews the origins and methodology behind BEC (Business Email Compromise) fraud in the real estate industry, the magnitude of loss stemming from this type of fraud, and current solutions for real estate professionals to prevent it from affecting their organization.

Fraud is an increasingly concerning issue in today's modern financial landscape. The real estate industry is particularly vulnerable, and is currently one the highest-targeted areas in which various forms of fraud occur. In 2017 alone, there were almost 10,000 victims of fraud in the real estate sector[1].

BEC Fraud - How Does it Work?

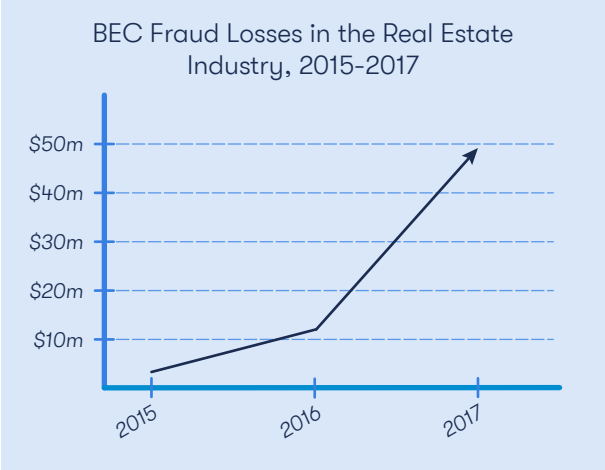
The most common form of fraud in the real estate industry is called business email compromise, and is frequently targeted at title companies and mortgage lenders. The basic premise of a BEC scheme is the impersonation of a trusted client, company executive, or supplier. This is similar to EAC (email account compromise), but instead of targeting individuals, it targets businesses or employees within a business. BEC relies on fooling a victim into believing that the attacker is a legitimate business associate and leading them to carry out an action to the attacker's benefit – most commonly initiating a wire transfer to an account owned by the attacker. In the real estate industry, this is often perpetrated within the context of a closing, as the amount of money needed to complete most transactions is a tempting target for criminals.

Because this type of fraud is most effective when the impersonation is accurate, it generally starts with an advance monitoring of a company's email traffic. First, the attacker will gain access to a company's network, either through forced entry or through social engineering. In many cases, the attacker will find a specific transaction and gather detailed Information relating to contacts, payment amounts, and scheduling. By doing so,

they can leverage these details to more effectively trick the victim into carrying out instructions on their behalf.

The second phase involves transmitting fraudulent wire instructions to the victim. This may come from a legitimate email address that the attacker has gained access to, or a spoofed email that is similar in appearance to a legitimate address.

The third phase is the actual execution of the unauthorized transaction requested by the attacker. The victim will, believing that the request is legitimate, carry out a wire transfer that will end up in a bank account owned by the attacker.



Losses from BEC Fraud in Recent Years

As technology develops, real estate transactions are completed at an ever-increasing pace. The reliance on email as a primary source of communication in the industry is of particular importance, as BEC fraud uses email as its main attack vector. These two factors combined explain the dramatic rise in this type of attack in the past few years.

The impact of BEC fraud is increasing exponentially. In 2017, the losses from these attacks totaled nearly $1 billion. Between the years of 2015 and 2017, the number of fraud reports increased by 1,100% in the real estate industry alone[2]. The dollar amount targeted by criminals was $5.3 billion in 2016[3]. It's worth noting that not all cases of fraud are reported – so the actual numbers may be much higher.

How to Recognize BEC Fraud

There are five major red flags that real estate professionals need to look out for when it comes to BEC fraud. The methodology behind these attacks are becoming more complex and more effective, so constant vigilance is required.

Unusual Requests

If a request comes through that seems out of the ordinary or is from someone unexpected, it may be an attempt at fraud - especially if the request is in the form of wiring instructions. Although not every step in a real estate transaction is set in stone, be cautious when faced with any instructions that contradict previously-established dates, amounts, or contacts.

Urgent or High-Pressure Requests

A heightened or unusual sense of urgency accompanying the request/instruction may also be a giveaway – it is a common tactic in pressuring the victim to wire out illegitimate funds. Because transactions move quickly in the real estate industry, it's important to stay aware in situations where urgency is being stressed - especially at end of month, a highly-targeted period for fraud attempts due to its hectic nature.

The 5 Red Flags of BEC Fraud

1. Unusual Requests
2. Urgency
3. Language Errors
4. Avoidance
5. Fake Email Address

Language

Be wary if the language of the person requesting a transfer is worded poorly or has misspellings. Although some criminals involved in these scams are well-spoken, many are not. Any strange phrasing, misspelled words, or punctuation errors may be an indication that the individual you are speaking with is not legitimate.

Avoidance

If the contact is refusing to speak verbally or is making excuses to avoid a phone conversation, there is a strong possibility it is an attacker. Verbal confirmation of wiring instructions is a common practice in the industry, so anyone refusing to do so could be considered suspect.

Incorrect Contact Information

Lastly and perhaps most importantly, if a request comes from an address that differs slightly from the contact's original address, it is fraudulent. Attackers will sometimes attempt to fool their victims by using an email address that very closely resembles the contact's actual address, thereby creating an opportunity to steal information or transmit fraudulent wiring instructions. This is commonly known as display name deception.

Over 75% of BEC attacks use display name deception rather than address spoofing[4]

Solutions for Preventing BEC

BEC does not happen spontaneously. In fact, most of the work involved actually occurs before any indication that a scam is taking place. It starts weeks or even months in advance, as attackers monitor email traffic to collect details on promising transactions. So in addition to keeping the above-listed red flags in mind, real estate professionals also need to stay vigilant when sharing any information related to an account or transaction. Try to avoid sharing any sensitive information electronically – verbal communication is always the best option. Likewise, be wary of requests for personal or financial information for "verification" purposes when it is abnormal to do so.

Keep in mind, however, that fraudulent actors with spoofed email addresses may include falsified phone numbers in an

email. Several reports over the past few years have noted that criminals may also employ phone calls to verify alternative payment instruction, posing as a legitimate contact[5]. One way to combat this is to only use phone numbers or email addresses that you have directly obtained from the parties in the transaction, instead of using contact info included in an email.

Another strategy is to establish code phrases early on in the transaction. By sharing these with trusted parties, you ensure that a change in payment instructions can be unequivocally verified.

Most importantly, do not initiate a wire transfer if there are any red flags present, even when you are being pressured to do so. Verification and security must take priority in these situations. Always confirm verbally with a known contact if you receive an unusual transfer request, or better yet, confirm with multiple parties when possible.

It isn't enough to simply provide this information to employees – a strict, enforceable policy must be implemented from the highest levels of an organization to ensure no one falls victim to BEC fraud. The reason why this type of fraud is so successful in the first place is because fraud prevention policies often take a back seat to the "crunch time" mentality that dominates the industry, especially at end of month. Therefore, security must be systemically treated with the utmost importance in order to effectively combat it.

In the event that a member of an organization does fall victim to BEC fraud, it is crucial that the incident be reported as soon as possible to authorities. While the recovery of stolen funds is never guaranteed, government financial crimes units have a much greater chance of doing so when fraud is reported within 24 hours of the incident[6].

There is another method for reducing instances of fraud attempt for lenders – third party fraud monitoring programs. Providers such as Ellie Mae® offer products that help to automate the fraud identification process, making it even harder for attackers to target your organization. Keep in mind, however, that this option does not completely eliminate the chances of fraud. Ultimately, the responsibility is on your organization's policies and personnel.

Conclusion

BEC fraud is an ever-growing threat in the real estate industry with thousands of cases and millions of dollars in losses reported each year. In order to effectively protect your organization, constant vigilance is required. Training employees to learn how to recognize the red flags of a BEC scam and adopting strict company-wide security policies are the best measures to ensure your organization will not fall victim.

References

1. Cronkright, Thomas, II. "Mortgage Lenders Must Step up to the Plate When It Comes to Wire Fraud." National Mortgage News. December 05, 2018. https://www.nationalmortgagenews.com/.

2. Yu, Melissa. "Mortgage Closing Scams: How to Protect Yourself and Your Closing Funds." Consumer Financial Protection Bureau. June 03, 2019. https://www.consumerfinance.gov/.

3. Murin, Joseph. "Sounding the Alarm: Mortgage Wire Fraud Is a Much Bigger Threat than You Realize." HousingWire. January 23, 2018. https://www.housingwire.com/.

4. "Business Email Compromise (BEC) Attack Trends Report." https://www.agari.com/bec/whitepapers/business-email-compromise-attacks-trends-report.pdf.

5. "Business Email Compromise: The 12 Billion Dollar Scam." Federal Bureau of Investigation Internet Crime Complaint Center (IC3). July 12, 2018. https://www.ic3.gov/media/2018/180712.aspx.

6. "Criminals Are Actively Using E-mail Schemes to Defraud Financial Institutions and Their Customers—billions of Dollars in Possible Losses." U.S. Treasury Financial Crimes Enforcement Network. September 6, 2016. https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003.

TIMIOS

TITLE & ESCROW SERVICES

At Timios, our goal is revolutionize and simplify the real estate transaction by placing the consumer in control of a totally transparent experience.

Learn more at www.Timios.com