LexisNexis®
RISK SOLUTIONS

Business Email Compromise in the Real Estate Sector: A Deeper Look into Trends and Solutions

Email has been relied on within the real estate industry for years to facilitate transactions between parties. And for good reason. It is a fast, convenient, accessible and cost-effective method of communication.

But email can provide an opportunity for social engineering tactics. Criminals find real estate closings to be a particularly attractive target due to the large sums of money involved. The industry's increased focus on more online and mobile transactions in lieu of in-person meetings has helped fuel an upsurge of business email compromise (BEC).

The problem of BEC has become so prevalent that it has caught the attention of the Financial Crimes Enforcement Network (FinCEN). A recent analysis determined that BEC incidents are a growing cybercrime concern for the real estate sector.[1] Discovering how to mitigate the challenges presented by BEC is key to defusing the activities of increasingly sophisticated criminals.

BEC is on the rise in the real estate sector

According to a recent report from wire fraud prevention firm CertifID, mortgage payoff fraud increased 532% between Q1 and Q2 2023.[2]

Increasing mortgage payoff fraud is likely also the result of a cooler housing market with fewer real estate transactions. Mortgage payoffs, which average more than $236,000, typically yield much higher payouts than wire fraud and are often initiated through a BEC.[3]

The cost and volume of mortgage-related fraud is particularly high for originators, servicers and title/settlement companies. Cyberattacks, such as wire fraud through BEC, are raising fraud levels even higher. Attempted attacks on title companies increased significantly, according to a 2022 survey by the American Land Survey Association. Nearly half of respondents (46%) state their employees receive at least one email a month attempting to change wire or payoff instructions.[4] The survey results used to produce the LexisNexis® Mortgage Lending Fraud Trends 2022 report have confirmed that fraud attacks increased significantly since the pandemic.

Why is BEC so successful?

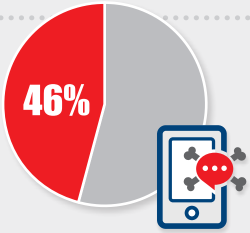
Perpetrators of BEC obtain unauthorized access to networks and systems to misappropriate confidential and proprietary information, such as a pending real estate sales transaction. At that point, criminals compromise the seller's email account or create a similar looking account and leverage social engineering (i.e., information about the transactions and parties involved). Typically, right before closing they send an email to gain trust and request to direct the settlement proceeds to a criminal controlled account.

A lack of frequent communication between mortgage servicers and title companies, as a result of breakdowns of processes and technology, also contribute to the problem. Too often, the fraud is not revealed until the seller receives a late payment notice from their lender on a loan they believed was paid off at closing. By then it becomes nearly impossible to recover the lost funds.

Mortgage payoff fraud increased

532%

between Q1 and Q2 2023.[2]



Nearly half of respondents (46%) state their employees receive at least one email a month attempting to change wire or payoff instructions.[4]

Who are the perpetrators of BEC?

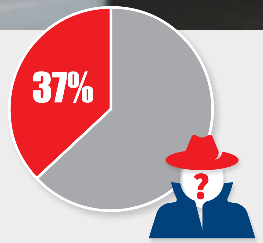
In BEC schemes, criminals frequently rely on third-party facilitators, including an increasing number of money mules. Carried out by transnational criminal organizations that employ hackers, social engineers and others, BEC can involve account compromise, key party impersonation, data theft and more.

FinCEN has recently observed an uptick of money mules who knowingly or unknowingly transfer or move illegally acquired funds following real estate BEC incidents.[5]

Who are BEC's prime victims?

Settlement and closing remain a prime target for BEC attacks exploiting the high monetary values generally associated with real estate transactions. Increasingly, the various communications between entities involved in the real estate title and closing processes (e.g., title companies, title agents, closing agents and escrow companies) have become susceptible to BEC attacks.

Of the 2,013 real estate BEC incidents during FinCEN's review period (from January 2020 to December 2021), 37% (or 743 incidents) involved title and closing entity impersonation.[6] Title/Settlement companies also reported in the LexisNexis® True Cost of Fraud™ Real Estate Study that for every $1 of fraud they incurred $4.91 in associated costs (i.e., labor, investigative, legal and external recovery related costs).[7] That means the true cost is nearly five times more than the lost closing proceeds. Relying on errors and omissions insurance policies is a temporary solution to recoup some of these costs before the resulting increased policy premiums become problematic.



Of the 2,013 real estate BEC incidents, **37% (or 743 incidents)** involved title and closing entity impersonation.[6]

For every $1 of fraud they incurred **$4.91 in associated costs.**[7]

BEC is an identity verification problem

In this information era, email fraud often becomes identity fraud because of lack of verification. In fact, FinCEN's analysis of the accounts involved in real estate BEC incidents during the review period indicates that fraudsters may be engaged in multiple types of fraud including identity fraud.

Identity verification remains a top challenge for mortgage originators, servicers and title/settlement companies. It contributes to other issues related to the inability to distinguish between legitimate and fake communications. In fact, title/settlement companies overwhelmingly rank verification of customer identity (91%) as their top-ranked fraud challenge.[8]

Smart practices to combat BEC

Combatting BEC requires robust identity proofing, including emails. With the growth of digital channels, leveraging email intelligence to assess risk is critical. BEC fraud is the reason we see much of the real estate industry investing in more secure communications platforms/capabilities for all communications related to a transaction.

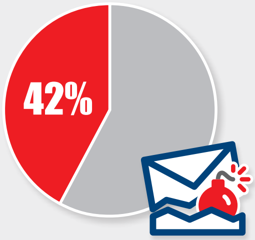
LexisNexis®
RISK SOLUTIONS

Leverage email intelligence to assess risk

LexisNexis® Emailage® is a powerful fraud risk scoring solution fueled by email intelligence as a core risk identifier. It leverages billions of digital identifiers, millions of fraud events and analyzes risk from billions of customer events to assess email risk while preserving a positive customer experience. It is a key component of our suite of award-winning anti-fraud solutions trusted by industries and governments.

Digital identifiers · Fraud events · Customer events

Emailage® Benchmark Statistic



Average Fraud Hit Rate – 42%
identified as high risk by Emailage and **turned out to be fraud.**[9]

Learn how you can deploy Emailage as part of a comprehensive security solution for fraud and identity management and better insulate against costly mortgage fraud losses without adding transaction delays.

For more information, call 800.957.7094

PAYMENT SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions includes seven brands that span multiple industries and sectors. We harness the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit risk.lexisnexis.com and www.relx.com.

[1] https://www.fincen.gov/sites/default/files/shared/Financial_Trend_Analysis_BEC_FINAL.pdf

[2-3] https://www.housingwire.com/articles/mortgage-payoff-fraud-rises-532-quarter-over-quarter-certifid/

[4] https://www.alta.org/news/news.cfm?20220810-Survey-Cyber-Attacks-Against-Title-Companies-Continues-to-Increase

[5-6] https://www.fincen.gov/sites/default/files/shared/Financial_Trend_Analysis_BEC_FINAL.pdf

[7-8] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#realestate

[9] Results are average and are based on multiple POCs done with new customers and incremental benefits received by existing customers. These may vary based on different geographies, customer inputs and industries.

LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.