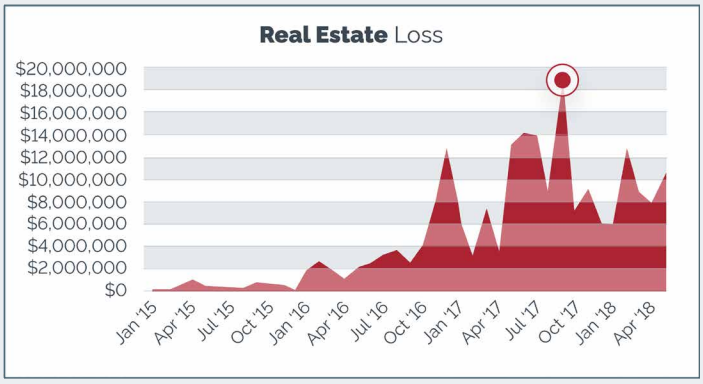
IDENTITYIQ®

NEW REAL ESTATE RISK: BUSINESS EMAIL COMPROMISE SCAMS

IdentityIQ.com
888-467-7102 Option 2
sales@idiqpartners.com

When buying or selling a new home, there are a number of factors to consider: property value, neighborhood crime statistics, public school system quality, taxes and more. Unfortunately for those involved in real estate transactions, another consideration can now be added to the list — the risk of becoming an identity theft victim during the home-buying process.

A Spike in Business Email Compromise Scams



Source: FBI Internet Crime Complaint Center

The rise in business email compromise (BEC) scams is of particular concern for the real estate industry. In fact, the real estate industry recently became the third-highest sector for BEC fraud.

According to the latest data by the FBI's new Internet Crime Complaint Center (IC3), the number of real estate-related BEC reports increased by almost **1,100%** in three years while the reported monetary loss increased by nearly **2,200%**.

What is BEC?

BEC along with e-mail account compromise is a sophisticated scam targeting both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting personally identifiable information (PII) or wage and tax statement (W-2) forms for employees.

The Phishing Problem

The Better Business Bureau reports BEC scams are especially challenging in real estate closings due to the variety of parties corresponding over email. In a typical real estate transaction, there can be up to 12 different stakeholders involved. As a result, a home buyer often receives fragmented communication from a variety of different individuals. A home buyer may view an email without noticing a minor discrepancy such as a single-letter difference in an email address from their real estate or title agent.

Victims participating at all levels of a real estate transaction have reported such activity to IC3. This includes title companies, law firms, real estate agents, buyers, and sellers. Victims most often report a spoofed e-mail being sent or received on behalf of one of these real estate transaction participants with instructions directing the recipient to change the payment type and/or payment location to a fraudulent account. The funds are usually directed to a fraudulent domestic account that quickly disperse through cash or check withdrawals. The funds may also be transferred to a secondary fraudulent domestic or international account. Funds sent to domestic accounts are often depleted rapidly, making recovery difficult.

SOLUTION

Educate Clients

A recent American Land Title Association (ALTA) study indicates that title and escrow companies may need to create more urgency around the threat of real estate scams. The study found that 73% of home buyers are warned about the threat of real estate fraud. But nearly half of the respondents, about 42%, said they are not concerned about identity theft during their real estate transaction.

Leaders at ALTA believe home buyers need more concrete, real-world examples of real estate fraud to tangibly understand the impact of BEC scams. They recommend title and escrow businesses do more than warn homebuyers about the threat of real estate scams; they must also provide incident reports and concrete examples to help home buyers understand the gravity of the issue and its far-reaching impact.

According to Michael Scheumack, a technology and marketing expert for IdentityIQ services, unaware home buyers can be particularly vulnerable to such scams, especially if they're doing much of their communication online or over the phone and sharing information like Social Security and bank account numbers. Mortgage professionals can play an important role in preventing these scams by educating their clients about the scams themselves and steps they can take to protect themselves.

Strengthen Security Systems

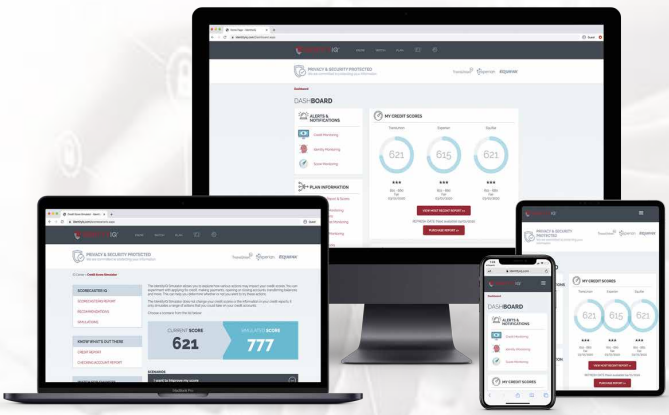
Title and escrow businesses can help secure PII by investing in best-in-class digital security. Title and escrow companies can do their due diligence to ensure their technology partners meet best practices and the highest standards for user data protection and security.

Use Portal-Based Communication for File Sharing

New portal-based communication is replacing traditional email communication as a more secure space for exchanging information. App-based portals can allow title and escrow businesses to securely communicate with home buyers, real estate agents, lenders, underwriters and other transaction party members in real-time, eliminating the need for fragmented email communication that can be intercepted by cybercriminals.

About **IdentityIQ**

Offered by IDIQ®, IdentityIQ® services are the solution for credit report and identity theft monitoring. Our team of experts utilizes innovative techniques for active credit report monitoring and identity theft protection, so you have financial peace of mind. An industry leader, IdentityIQ services have been named to the Inc. 5000 list of the fastest-growing companies in the United States by "Inc." magazine and "50 Most Valuable Brands of the Year" by "The Silicon Review". For more information, visit IdentityIQ.com.



SOURCES:
Financial Crimes Enforcement Network/FinCEN;
FBI Internet Crime Complaint Center;
Better Business Bureau; and
American Land Title Association

For more information, visit idiq.com and identityiq.com.