First American Title™
NATIONAL COMMERCIAL SERVICES

Protect yourself from Cyber Fraud

CYBER FRAUD AWARENESS GUIDE

A Growing Problem

It was the year the FBI's Internet Crime Complaint Center (IC3) received its 4 millionth consumer Internet crime complaint.[1]

It was the year the IC3 received a total of 301,580 complaints, with reported losses exceeding $1.4 billion.[1]

2017 was certainly a milestone year for the FBI's IC3. By volume, the top three crimes reported were non-payment / non-delivery, personal data breach and phishing.[1]

For the title and settlement services industry, Business Email Compromise (BEC) / Email Account Compromise (EAC) was the top crime last year, with the highest reported loss at more than $675 million.[1]

BEC is a sophisticated scam targeting businesses that regularly perform wire transfer payments. The EAC variation of BEC targets individuals who regularly perform wire transfer payments, such as title agents and escrow officers.

Cyber fraud is real. So it's important to remain vigilant and up to date, knowing the best ways to protect yourself and your business.

Business Email Compromise (BEC) & Email Account Compromise (EAC) Scams

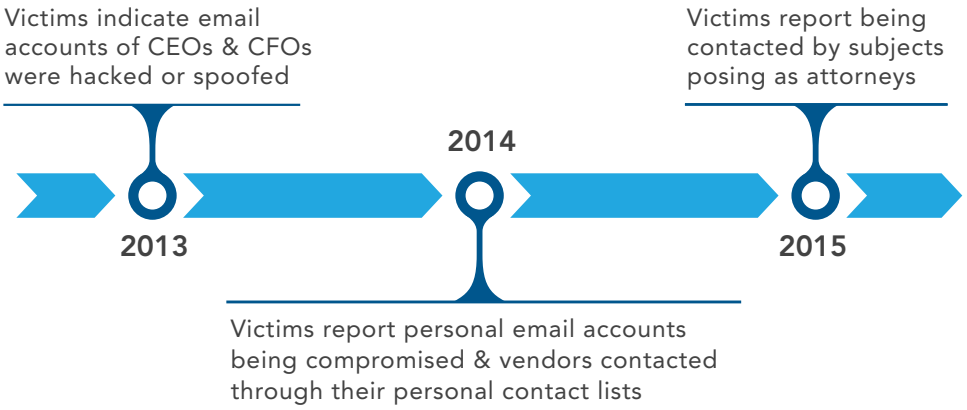
Both scams typically involve one or more fraudsters who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The techniques used in the BEC and EAC scams have become increasingly similar, so the FBI's IC3 began tracking these scams as a single crime type in 2017.[1]

Fraudulent transfers conducted as a result of BEC and EAC have been routed through accounts in many countries, with a large majority traveling through Asia.[1]

BEC and EAC scams are constantly evolving as scammers become more sophisticated. The following timeline outlines the growing sophistication and approach of fraudsters:[1]

Timeline: Increasing Sophistication of Fraudsters



2013 – HIGH-LEVEL EXECUTIVES TARGETED

Victims of BEC and EAC indicated email accounts of chief executive officers or chief financial officers were hacked or spoofed, resulting in fraudulent emails requesting wire payments to be sent to fraudulent locations.

2014 – IT GETS PERSONAL

Victims reported personal email accounts were being compromised, and fraudulent requests for payment were sent to vendors identified through their personal contact lists.

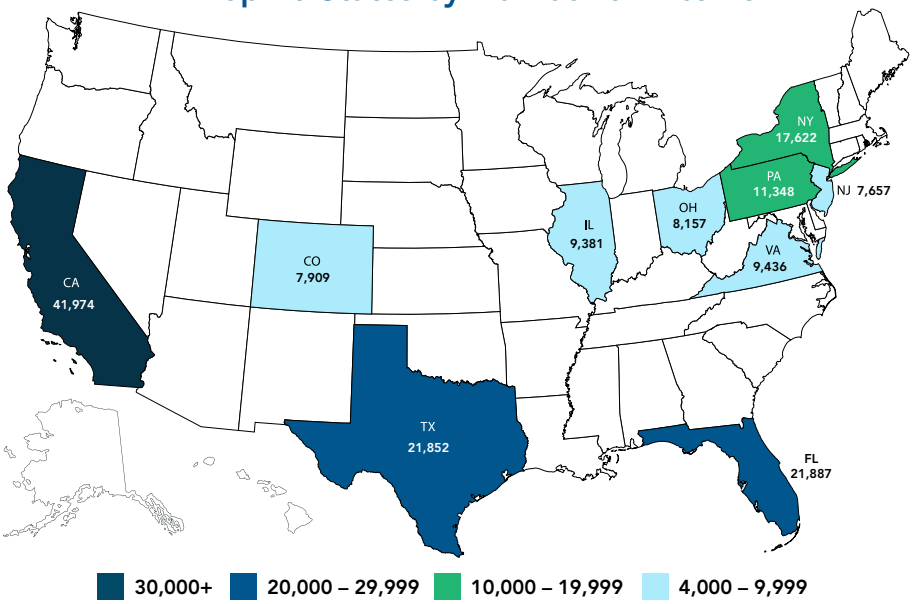
[1] FBI INTERNET CRIME COMPLAINT CENTER (IC3) 2017 INTERNET CRIME REPORT

2015 – FRAUDSTERS POSE AS LAWYERS

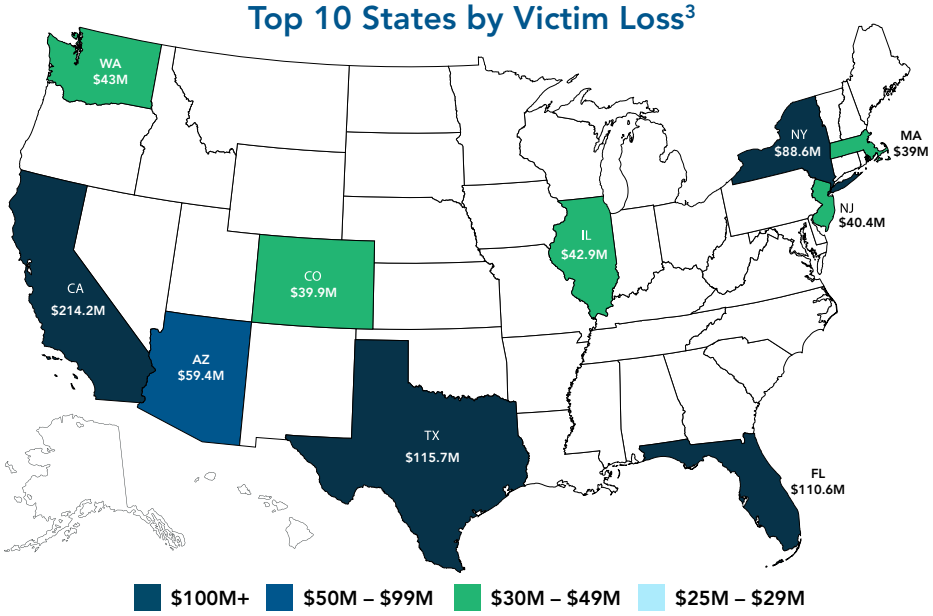
Victims reported being contacted by subjects posing as lawyers or law firms instructing them to make secret or time-sensitive wire transfers.

Cyber Fraud is an Issue Across the Nation

Top 10 States by Number of Victims[2]



Top 10 States by Victim Loss[3]



Source: FBI 2017 Internet Crimes Report

[2] Accessibility description: image depicts the United States, with the top ten states (based on reported victims) highlighted. These include California (41,974), Florida (21,887), Texas (21,852), New York (17,622), Pennsylvania (11,348), Virginia (9,436), Illinois (9,381), Ohio (8,157), Colorado (7,909), and New Jersey (7,657).

[3] Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California ($214.2M), Texas (115.7M) Florida ($110.6M), New York ($88.6M), Arizona ($59.4 M), Washington ($43M), Illinois ($42.9M), New Jersey ($40.4M), Colorado ($39.9M), and Massachusetts ($39M).

How Fraud Works in Title & Settlement Services Transactions

Real estate transactions involve a significant amount of personal information. Everyone involved – from buyers / sellers to real estate professionals, attorneys and title / settlement companies – must be exceptionally diligent in protecting that information.

In real estate transactions, fraudsters assume the identity of the title agent, escrow officer or real estate agent handling the sale. The criminals forge the person's work email and other details that appear specific and authentic. Next – posing as the real estate agent, title agent or escrow officer – the scammers send an email to the buyer or the lender that includes wire instructions to send the funds to the criminal's bank account.[4]

Now that you know what types of fraud the commercial real estate industry is facing, it's time to look into proactive ways to protect your company and transactions.

The Best Protection is Knowledge — Be Cyber Secure with these Proactive Email Security Tips

Email Security Tips

Cyber fraud is on the rise, largely due to compromised email accounts being used to initiate wire fraud and other financial crimes. For every company, the first step is to discuss prevention and processes with your Information Technology department to understand and follow your company procedures.

The following security tips, which may be similar to recommendations from your company's IT department, can help you identify a compromised email account and prevent further exploitation.

PROTECT YOUR EMAIL ACCOUNT

- Change your password often. Make it complex, and avoid using personal information.
- Enable two-factor authentication for account access. A quick Internet search will show how to set this up for most major email providers.
- Maintain and routinely update an anti-virus/malware program.
- Scrutinize email content, and avoid anything that looks suspicious.
- Before you click a URL, hover your cursor over the sender's email address along with any URLs in the message to be sure they are legitimate.
- If you suspect the 'From' address is fraudulent, you can check it with a header analyzer, such as one offered by Google.
- Review your account activity records for suspicious logins.
- Periodically check your Sent folder to be sure emails aren't being sent or forwarded without your knowledge.
- Periodically check your email configuration to ensure automatic forwarding has not been enabled without your knowledge. A quick Internet search will show you how to configure forwarding for most major email providers.

INDICATORS THAT AN EMAIL ACCOUNT HAS BEEN COMPROMISED

- You are unable to log in, indicating your password has been changed.
- Activity records show suspicious login times or unknown locations.
- Account configuration is set to forward emails to an unknown address.
- Friends and/or colleagues are receiving "spam" messages from your account.
- You receive replies to emails you didn't send.

[4] FBI: BUSINESS EMAIL COMPROMISE TOPS ONLINE FRAUD LOSSES IN 2017, ALTA TITLE NEWS ONLINE, JUNE 7, 2018

TIPS TO RECOVER A COMPROMISED EMAIL ACCOUNT

- Change your password immediately.
- If possible, make the account disconnect or sign out of other web sessions.
- Check the message forwarding settings to ensure hackers are not being forwarded incoming emails.

Note that a compromised email account could be an indicator that the computer itself has been hacked. It is recommended that users complete a full virus scan and change the computer login password.

Additional Thoughts about Protection: Awareness of Your Connections

The real estate industry has been plagued by incidents of email-related fraud in which closing funds, sales proceeds and other monetary transfers are rerouted to criminals. These email fraud scenarios are clever, varied and devious.

Protection of information is at the heart of preventing this type of fraud. Many people are used to protecting sensitive information like their social security number or bank account, but online accounts could be the key to unlocking enough information for a criminal to stage an impersonation.

PROTECTION BEGINS WITH AN AWARENESS OF:

- Where you connect – home, work, on the go.
- How you connect – your computer and mobile devices.
- Your security authentication for connection – the appropriate use of passwords and multi-factor authentication.

Cyber Security Methods

DEVICES

- Ensure the operating system, security software, browsers and apps are up to date on your computer and mobile devices. Protect all devices that connect to the Internet, including gaming systems and other web-enabled devices.
- Delete unused or defunct apps.
- Minimize the information accessible by apps.
- Prevent unauthorized access to mobile devices by using passcodes or other authorization methods (fingerprint scanning, pattern recognition, etc.)
- Deactivate Wi-Fi and Bluetooth when not in use to prevent unauthorized access while you're on the go.
- Educate all business associates and family members about cyber security. It only takes one user to infect a network of devices.

PASSWORD AND ACCESS

- Use strong passwords that include a mix of characters (upper and lowercase, numbers, special characters). Rather than using a single word, make your password a sentence or phrase. Avoid using any personal information like a birthday or child's name.
- Be aware of what you share. Your password should not be linked to anything that you share publicly or on social media. If you always talk about your love of chocolate online, your password should not be iLOVEch0colate!
- Use a different password for each important account, such as banking, email, social media and other accounts that are prone to attack. Criminals may breach one account and then use your password to access others.
- If any online account offers multi-factor authentication, use it. This means the user must be identified by multiple methods for access or password resets. For instance, an account may send a code to your phone or email address and you must enter the code to gain access to the account, in addition to entering a password.

BEHAVIOR

- Don't click on any links or open attachments unless you trust the source.
- If you receive email communication concerning the delivery of funds on a real estate transaction, call the sender at a trusted phone number – not a phone number listed in the email.

Resources

How to Submit a Complaint if You Become a Victim of Fraud

Victims of email fraud can submit a complaint via the FBI's Internet Crime Complaint Center site.

Additional information to help protect yourself from malicious emails can be found in the SANS Security Awareness Newsletters.

Contact your email service provider for more information and tips to protect your important communications.

Visit the Consumer Financial Protection Bureau Fraud and Scams Information for helpful tools.

Visit the FBI Scam and Safety Information website.

First American Title National Commercial Services is committed to protecting your information.

Thank you for joining us in fostering a secure electronic environment for your real estate transactions and more.