Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 09, 2023

Alert Number
I-060923-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise: The $50 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-050422-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2022.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. Often times BEC variations involve compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, and crypto currency wallets.

STATISTICAL DATA

The BEC scam has continued to evolve, targeting small local businesses to larger corporations, and personal transactions. Between December 2021 and December 2022, there was a 17% increase in identified global exposed losses. In 2022, the IC3 saw an increase in BEC reporting with a nexus to the real estate sector and BEC incidents where funds were transferred directly to a cryptocurrency exchange, or to a financial institution holding a custodial account for a cryptocurrency exchange. (See also: PSA I-041321-PSA)

The BEC scam has been reported in all 50 states and 177 countries, with over 140 countries receiving fraudulent transfers. Based on the financial data reported to the IC3 for 2022, banks located in Hong Kong and China were the primary international destinations of fraudulent funds. These were followed by the United Kingdom, which often acts as an intermediary stop for funds, Mexico, and Singapore.

The following BEC statistics were reported to the FBI IC3, law enforcement and derived from filings with financial institutions between **October 2013 and December 2022**:

Domestic and international incidents: **277,918**
Domestic and international exposed dollar loss: **$50,871,249,501**

The following BEC statistics were reported in victim complaints to the IC3 between **October 2013 and December 2022**:

Total U.S. victims: **137,601**
Total U.S. exposed dollar loss**:** **$17,328,435,141**

Total non-U.S. victims**:** **5,892**
Total non-U.S. exposed dollar loss: **$1,454,028,296**

The following BEC statistics were reported by victims via the financial transaction component of the IC3 complaint form, which became available in June 2016. The following statistics were reported in victim complaints to the IC3 between **June 2016 and December 2022**:

Total U.S. financial recipients: **74,121**
Total U.S. financial recipient exposed dollar loss**:** **$13,034,596,130**

Total non-U.S. financial recipients: **21,122**
Total non-U.S. financial recipient exposed dollar loss: **$8,451,345,479**

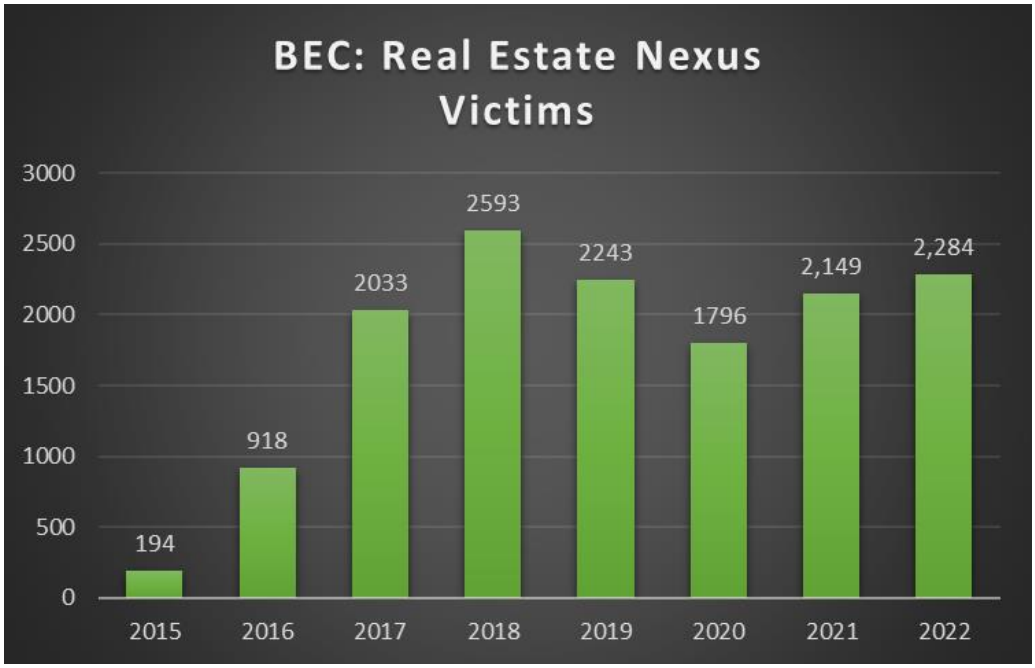
BEC Highlights: Real Estate Sector

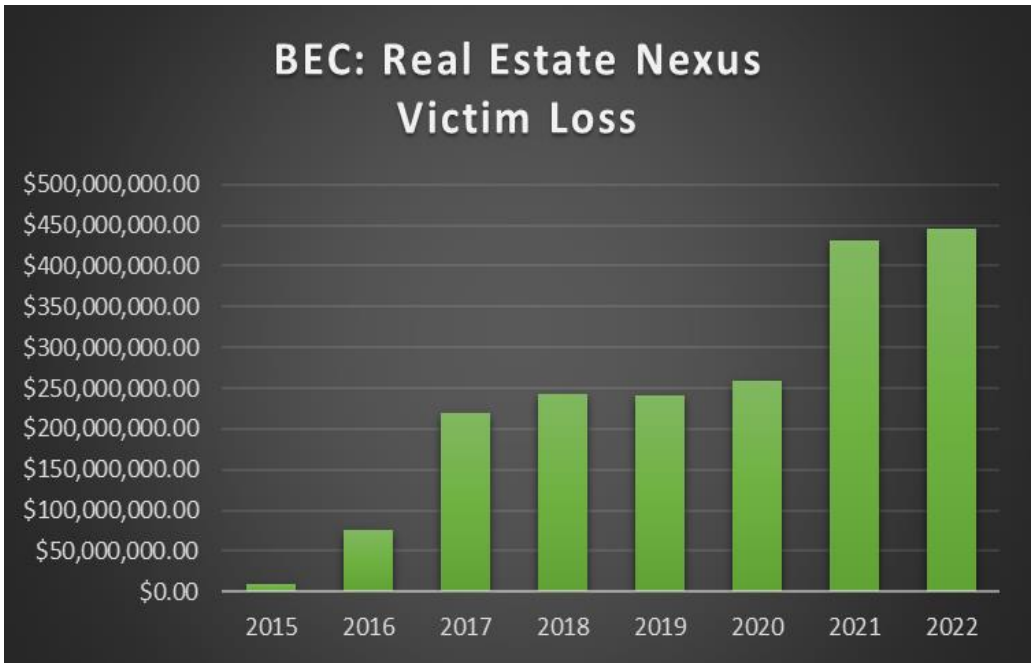
In calendar year 2018, reporting to the IC3 for BEC with a nexus to the real estate sector was at an all-time high. Gradually, reporting to the IC3 decreased in the following years until another minor spike in 2021 and then again increasing in 2022.

The BEC scam targets all participants in real estate transactions, to include buyers, seller, real estate attorneys, title companies, and agents. Once a BEC perpetrators gain access to a participant's email account involved in a real estate transaction, they are able to monitor the real estate proceeding and often time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one bank account to a different bank account under their control. The funds may also be transferred to a secondary fraudulent domestic or international account.

Based on IC3 victim complaint data, BEC scams targeting the real estate sector are once again on the rise. From calendar years 2020 to 2022, there was a 27% increase in victim reports to the IC3 of BECs with a real estate nexus. In this same time frame, there was a 72% increase in victim loss of BECs with a real estate

nexus. The increases in victim losses of BEC with a real estate nexus are notable with the increase in victim reporting and also may be contributed to the rise in real estate costs over the last several years.





Federal Bureau of Investigation
Public Service Announcement

SUGGESTIONS FOR PROTECTION

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

If you discover a fraudulent transfer, time is of the essence. **First**, contact your financial institution and request a recall of the funds along with any necessary indemnification documents. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds. Regardless of the amount lost, file a complaint with www.ic3.gov , as soon as possible. The FBI IC3 will be able to assist both the financial institutions and law enforcement in possible recovery efforts.