Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-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 $43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) 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. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, or even crypto currency wallets.

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small local businesses to larger corporations, and personal transactions. Between July 2019 and December 2021, there was a 65% increase in identified global **exposed losses**, meaning the dollar loss that includes both actual and attempted loss in United States dollars. This increase can be partly attributed to the restrictions placed on normal business practices during the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

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 2021, banks located in Thailand and Hong Kong were the primary international destinations of fraudulent funds. China, which ranked in the top two destinations in previous years, ranked third in 2021 followed by Mexico and Singapore.

The following BEC/EAC statistics were reported to the FBI IC3, law enforcement and derived from filings with financial institutions between **June 2016 and December 2021**:

Domestic and international incidents:	**241,206**
Domestic and international exposed dollar loss:	**$43,312,749,946**

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and December 2021:**

Total U.S. victims:	**116,401**
Total U.S. exposed dollar loss:	**$14,762,978,290**
Total non-U.S. victims:	**5,260**
Total non-U.S. exposed dollar loss:	**$1,277,131,099**

The following statistics were reported in victim complaints to the IC3 between **June 2016 and December 2021:**

Total U.S. financial recipients:	**59,324**
Total U.S. financial recipient exposed dollar loss:	**$9,153,274,323**
Total non-U.S. financial recipients:	**19,731**
Total non-U.S. financial recipient exposed dollar loss:	**$7,859,268,158**

BEC AND CRYPTOCURRENCY

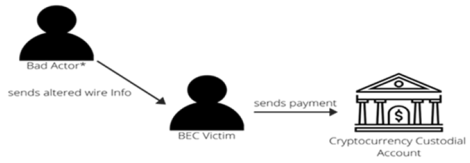
The IC3 has received an increased number of BEC complaints involving the use of cryptocurrency. Cryptocurrency is a form of virtual asset that uses cryptography (the use of coded messages to secure communications) to secure financial transactions and is popular among illicit actors due to the high degree of anonymity associated with it and the speed at which transactions occur.

The IC3 tracked two iterations of the BEC scam where cryptocurrency was utilized by criminals. A direct transfer to a cryptocurrency exchange (CE) or a "second hop" transfer to a CE. In both situations, the victim is unaware that the funds are being sent to be converted to cryptocurrency.

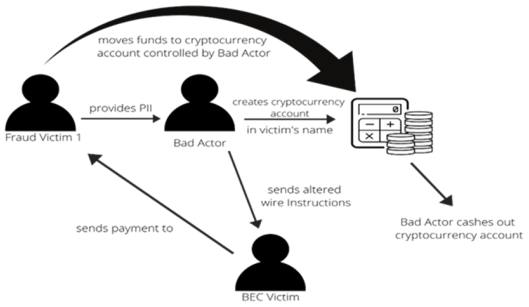
DIRECT TRANSFER – Mirrors the traditional pattern of BEC incidents in the past.

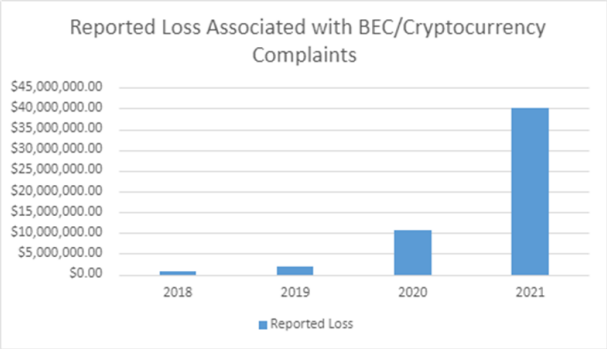
SECOND HOP TRANSFER - Uses victims of other cyber-enabled scams such as Extortion, Tech Support, and Romance Scams. Often, these individuals provided copies of identifying documents such as driver's licenses, passports, etc., that are used to open cryptocurrency wallets in their names.

In the past, the use of cryptocurrency was regularly reported in other crime types seen at the IC3 (e.g., tech support, ransomware, employment), however, it was not identified in BEC-specific crimes until 2018. By 2019, reports had increased, culminating in the highest numbers to-date in 2021 with just over $40M in exposed losses. Based on the increasing data received, the IC3 expects this trend to continue growing in the coming years.



*Bad Actor has already arranged control of a named cryptocurrency wallet for the funds to be converted to





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 you are the victim of a fraud incident, immediately contact your financial institution to request a recall of funds. Regardless of the amount lost, file a complaint with www.ic3.gov or, for BEC/EAC victims, BEC.ic3.gov, as soon as possible.