Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-091124-PSA
September 11, 2024

Business Email Compromise: The $55 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-060923-PSA posted on www.ic3.gov. This PSA includes new IC3 complaint information and updated statistics from October 2013 to December 2023.

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 (PSA I-041124-PSA) or computer intrusion to conduct unauthorized transfers of funds. Often times BEC variations involve compromising legitimate business email accounts and requesting employees' Personally Identifiable Information in order to compromise other accounts that may be related to other scams.

STATISTICAL DATA

The BEC scam continues to target small local businesses to larger corporations, and personal transactions while evolving in their techniques to access those business or personal accounts. Between December 2022 and December 2023, there was a 9% increase in identified global exposed losses. In 2023, the IC3 saw a growth in BEC reporting where funds were sent directly to a financial institution housing custodial accounts held by third-party payment processors, or peer-to-peer payment processors, and cryptocurrency exchanges (PSA I-041321-PSA and PSA I-082423-PSA) which directly contributed to the increase in global exposed losses.

IC3 data shows the BEC scam has been reported in all 50 states and 186 countries, with over 140 countries receiving fraudulent transfers. Based on the financial data reported to the IC3 for 2023, international banks located in the United Kingdom and Hong Kong often acted as an intermediary stop for funds, followed by China, Mexico, and the UAE.

The following BEC statistics were reported to the FBI IC3, law enforcement and derived from filings with financial institutions between **October 2013 and December 2023:**

Domestic and international incidents:	**305,033**
Domestic and international exposed dollar loss:	**$55,499,915,582**

The following BEC statistics were reported in victim complaints to the IC3 between **October 2013 and December 2023:**

Total U.S. victims:	**158,436**
Total U.S. exposed dollar loss:	**$20,089,561,364**
Total non-U.S. victims:	**6,546**
Total non-U.S. exposed dollar loss:	**$1,638,490,375**

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 2023:**

Total U.S. financial recipients:	**89,756**
Total U.S. financial recipient exposed dollar loss:	**$17,499,104,054**
Total non-U.S. financial recipients:	**22,190**
Total non-U.S. financial recipient exposed dollar loss:	**$8,953,920,759**

HOW TO PROTECT YOURSELF/BUSINESS

If you discover a fraudulent transfer, time is of the essence. Immediately 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 may be able to assist both the financial institutions and law enforcement in freezing funds.

RECOMMENDED PREVENTION TIPS

- Use secondary channels and/or two-factor authentication to verify requests for changes in account information.
- Use unique passwords/passphrases. Make sure to use a unique password for every online service you use and try to change your passwords/passphrases periodically.
- 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 personal identifiable information (PII) of any sort via email. Be aware that many emails requesting your PII 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.