BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) 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.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses[2]. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries.

Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018:**

Total U.S. victims:	41,058
Total U.S. victims:	$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	$671,915,009

The following BEC/EAC statistics were reported by victims via the financial transaction component of the IC3 complaint form, which became available in June 2016[3]. The following statistics were reported in victim complaints to the IC3 from **June 2016 to May 2018:**

Total U.S. financial recipients:	19,335
Total U.S. financial recipients:	$1,629,975,562
Total non-U.S. financial recipients:	11,452
Total non-U.S. financial recipients exposed dollar loss:	$1,690,788,278

REAL ESTATE SECTOR TARGETS

BEC/EAC actors heavily targeted the real estate sector in recent years. 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 which 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.

Domestic money mules[4] are frequently identified in connection with the BEC/EAC real estate trend. BEC/EAC actors often recruit money mules through confidence/romance scams. The BEC/EAC actor may groom a victim and then direct them to open accounts under the guise of sending or receiving funds as directed by the BEC/EAC actor. The accounts opened to facilitate this activity are typically used for a short period of time. Once the account is flagged by the financial institutions, it may be closed and the BEC/EAC actor will either direct the romance/scam victim to open a new account or move on to grooming a new victim.

Based on victim complaint data, BEC/EAC scams targeting the real estate sector are on the rise. From calendar year 2015 to calendar year 2017, there was over an 1100% rise in the number of BEC/EAC victims reporting the real estate transaction angle and an almost 2200% rise in the reported monetary loss.[5] May 2018 reported the highest number of BEC/EAC real estate victims since 2015, and September 2017 reported the highest victim loss.

SUGGESTIONS FOR PROTECTION

BEC/EAC actors have been known to target all parties in a real estate transaction. The best defense is to verify all requests for a change in payment type and/or location. BEC/EAC actors often request that payments originally scheduled for check dispersal be made via wire instead. BEC/EAC actors may also request changes to the original recipient's financial information.

BEC/EAC actors will use information that is publicly available on real estate listing sites to target victims. This may include homes that are for sale and the progress of the sale such as "under contract" as well as the contact information of the real estate agent. Be wary of any communication that is exclusively e-mail based and establish a secondary means of communication for verification purposes.

Be mindful of phone conversations. Victims have reported receiving phone calls from BEC/EAC actors requesting personal information for verification purposes. Financial institutions report phone calls acknowledging a change in payment type and/or location. Some victims report they were unable to distinguish the fraudulent phone conversation from legitimate conversations. One way to counter act this fraudulent activity, is to establish code phrases that would only be known to the two legitimate parties.

Title Companies report establishing new procedures when processing legal documents requiring all changes in payment type and/or location to be verified prior to distributing funds.

If you discover a fraudulent transfer, time is of the essence. First, contact your financial institution and request a recall of the funds. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds. Second, contact your local FBI office and report the fraudulent transfer. Law enforcement may be able to assist the financial institution in recovering funds. Finally, regardless of dollar loss, file a complaint with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov. The IC3 will be able to assist both the financial institutions and law enforcement in the recovery efforts.

---

1. Reference PSA 1-022118-PSA Increase in W-2 Phishing Campaigns
2. Exposed dollar loss includes actual and attempted loss in United States dollars.
3. "Financial Recipient" is defined as an account holder who receives the fraudulent funds.
4. Money mules are defined as persons who transfer money illegally on behalf of others.
5. Based on IC3 adjusted loss