Financial Trend Analysis

Financial Crimes Enforcement Network / FinCEN

Manufacturing and Construction Top Targets for Business Email Compromise

July 2019

Financial Trend Analysis

Financial Crimes Enforcement Network / FinCEN

Manufacturing and Construction Top Targets for Business Email Compromise

The Financial Crimes Enforcement Network (FinCEN) is releasing this strategic analysis of Bank Secrecy Act (BSA) reporting to share relevant information with the public, including consumers, media, and a wide range of businesses and industries. The report also highlights the value of BSA information collected by regulated financial institutions. ***This document does not introduce a new regulatory interpretation, nor impose any new requirements on regulated entities****. The research detailed in this report is one of many examples of how FinCEN and its law enforcement, regulatory, and national security partners may analyze and use BSA reporting, but is not intended as guidance for financial institutions. For formal guidance to financial institutions on reporting business email compromise (BEC) incidents, please refer to FinCEN's resource page on advisories, at* https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets.

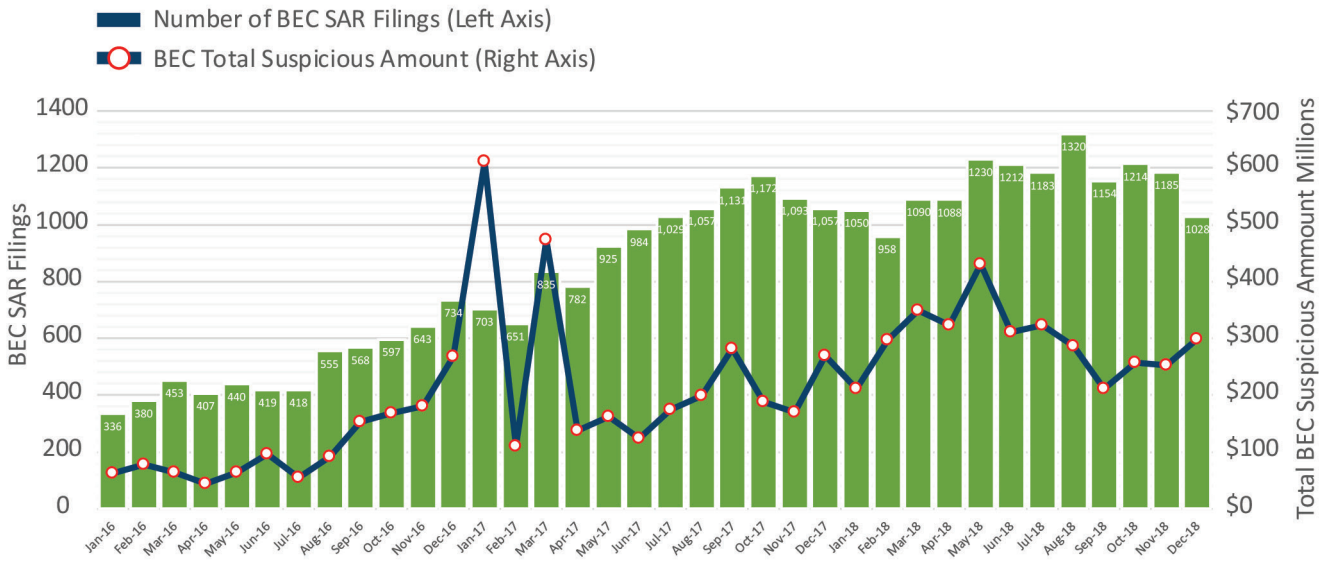
Executive Summary: The number of suspicious activity reports (SARs) describing business email compromise (BEC) incidents reported monthly has grown rapidly, averaging nearly 500 per month in 2016, and above 1,100 per month in 2018. The total value of attempted BEC thefts, as reported in SARs, climbed to an average of $301 million per month in 2018 from only $110 million per month in 2016. For portions of this report, FinCEN analyzed randomly selected, statistically representative samples of SAR narratives on BEC incidents filed in 2017 and 2018, to assess BEC trends and methods.

- Manufacturing and construction was the most targeted sector in both 2017 and 2018, representing 20 percent of all analyzed transactions in 2017 and 25 percent in 2018. Commercial services (such as shopping centers, entertainment facilities, and lodging) increased more than other industries, up from 6 percent of reported incidents in 2017 to 18 percent in 2018.
- In approximately 73 percent of incidents in 2017, funds were sent or attempted to be sent to domestic accounts, likely controlled by money mules. These destinations likely represent intermediate hops in a money laundering process, based on FinCEN's analysis of BEC networks and recent law enforcement insights on use of money mules in other scams.
- BEC scam methods have evolved over time. For example, impersonating a CEO or other high-ranking business officer accounted for 33 percent of sampled incidents in 2017, declining to 12 percent in 2018, while impersonation of an outside entity was 20 percent of 2018 reports, from an unmeasured amount in 2017. Using fraudulent vendor or client invoices grew, from 30 percent of sampled 2017 incidents, to 39 percent in 2018.

What is BEC?

BEC is a type of scam that targets businesses (and other types of organizations, such as educational institutions, government, and non-profits) and their fund transfers. Scammers generally target organizations that conduct large wire transfers in the course of their usual business and rely on email for much of their communication regarding the wires. Recent reporting indicates that other financial products, such as convertible virtual currency, automated clearing house transfers, and gift cards, can be used in BEC schemes.[1] The perpetrators typically compromise a key email account by using computer intrusions or social engineering and send an email that fraudulently directs funds to criminal-controlled accounts.[2] Perpetrators may use methods such as spear phishing, specialized malware, and spoofed emails. Often, the victim is tricked into thinking a legitimate email from a trusted person or entity is directing them to make a payment for a normal business activity.

Figure 1. Monthly BEC SAR Filings and Total Suspicious Transaction Amount



A review of SARs filed since 2016 identified a growing trend of reported BEC activity following the publication of the FinCEN Advisory FIN-2016-A005 on 25 October 2016. In 2016, financial institutions filed nearly 6,000 BEC-related SARs with an average transaction total of $110 million per month. In 2017, the number of BEC-related SARs increased to over 11,000 with a monthly average of $241 million. In 2018, the number of BEC-related SARs rose to nearly 14,000 filings, averaging $301 million in suspicious transactions per month. These figures closely

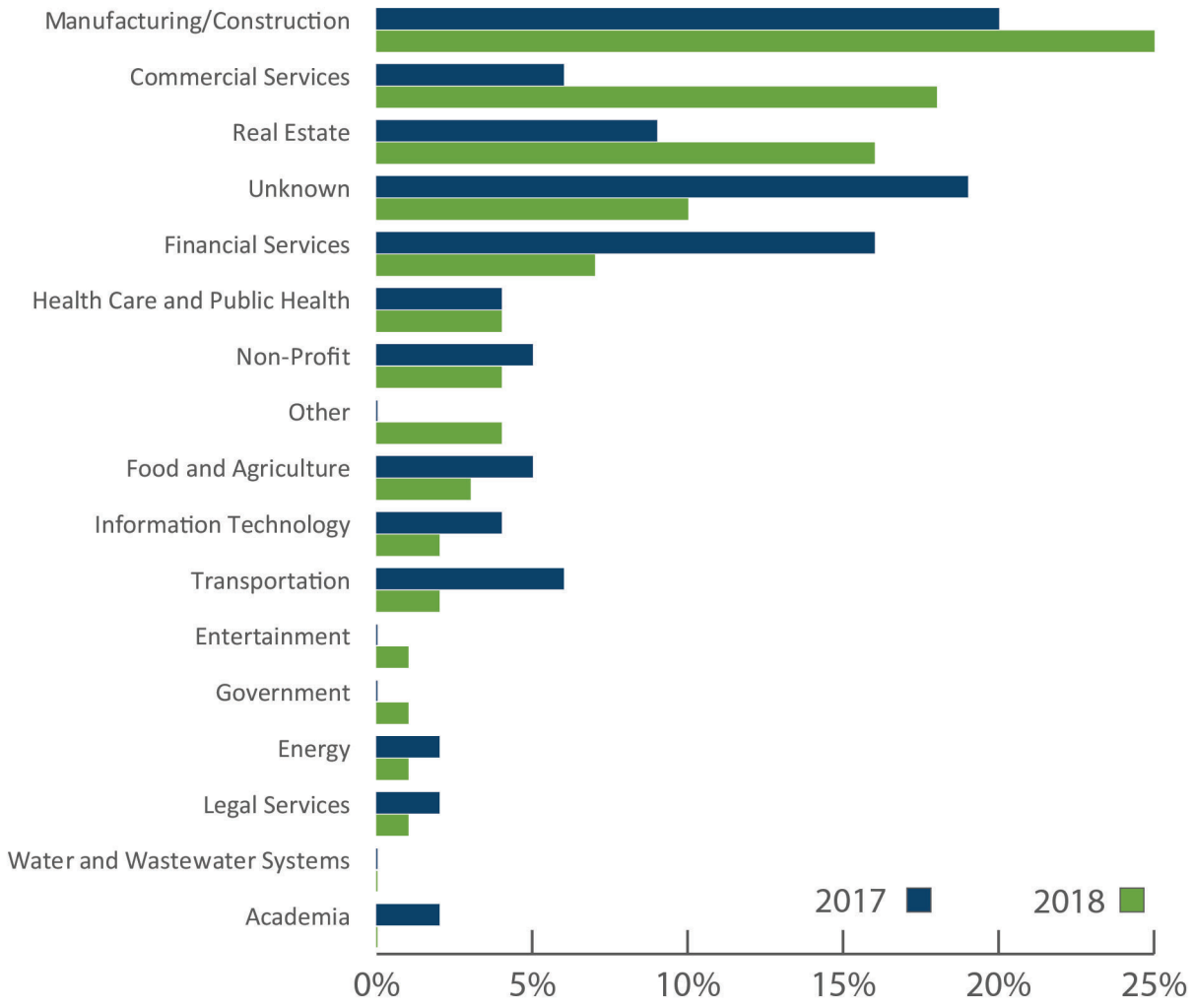
1. Financial Crimes Enforcement Network, draft "Updated Advisory to Financial Institutions on Email Compromise Fraud Schemes," reviewed 27 June 2019.
2. Financial Crimes Enforcement Network, "Advisory to Financial Institutions on Email Compromise Fraud Schemes" FinCEN Public Advisory #FIN-2016-A003, 6 September 2016, https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

correlate to public reporting from the FBI showing a 136 percent increase in "identified global exposed losses" between December 2016 and May 2018.[3] FBI indicates in the report that it considers "exposed" losses to be actual losses and attempted thefts.

Manufacturing and Construction Firms are Top BEC Targets

Manufacturing and construction businesses were the top targeted sector for BEC fraud in 2017 and 2018, accounting for 20 percent of all reported BEC incidents in 2017 (with an average fraudulent transaction amount of $53,728), and 25 percent in 2018. Commercial services (such as professional services companies like landscaping, retail, restaurants, and lodging) increased more than other industries, up from 6 percent of reported incidents in 2017 to 18 percent in 2018. Financial firms fell significantly in the rankings, from 16 percent in 2017 to 9 percent in 2018, while real estate firms increased, from 9 percent in 2017 to 16 percent in 2018.

Figure 2. 2017 and 2018 BEC Targets by Industry



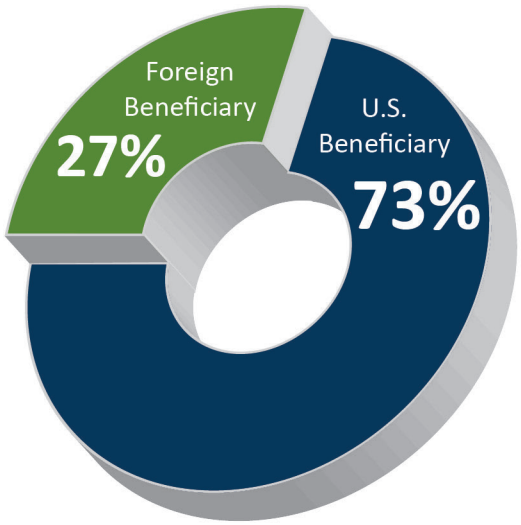
3. Federal Bureau of Investigation, Public Service Announcement I-071218-PSA, "Business Email Compromise: The 12 Billion Dollar Scam," 12 July 2018, https://www.ic3.gov/media/2018/180712.aspx, accessed 18 June 2019.

Among transactions targeting manufacturing and construction firms in 2017, 33 percent listed a foreign beneficiary. Regular interactions with overseas suppliers, who may require regular use of wire transfers for payment, and publicly available client information likely make manufacturing and construction companies particularly susceptible to BEC fraud.

Frequent high-dollar transactions in the real estate industry along with the improving real estate market most likely continued to make real estate an attractive target for perpetrators of BEC fraud in 2017 and 2018. While real estate firms represented 9 percent of all targeted firms in 2017, they accounted for over 20 percent of fraudulent transaction amounts. Real estate firms have the highest average fraudulent transaction amount of $179,001.

U.S. Accounts are the Top Destinations for BEC Proceeds

Figure 3. Domestic and Foreign BEC Beneficiaries



The overwhelming majority (73 percent) of BEC incidents reported in 2017 involved domestic transfers, likely taking advantage of "money mule" networks[4] across the United States to move stolen funds. Industries that are common in a particular state likely represent the most targeted companies in that state. For example, financial firms are the most frequently targeted firms in New York, while manufacturing and construction firms are the most frequently targeted in Texas. (Texas is ranked second in the United States after California for the state with the highest number of manufacturing jobs—847,000.)[5]

4. "Money mules" are individuals who transfer money on behalf of the BEC perpetrators. These individuals may be witting or unwitting participants in laundering BEC proceeds. Money mules are often recruited online through other scams.

5. Patricia Panchak, "California Unseats Texas as Top IW US 500 Manufacturing State," Industry Week, 8 July 2016, https://www.industryweek.com/industryweek-us-500/california-unseats-texas-top-iw-us-500-manufacturing-state, accessed 9 October 2018.

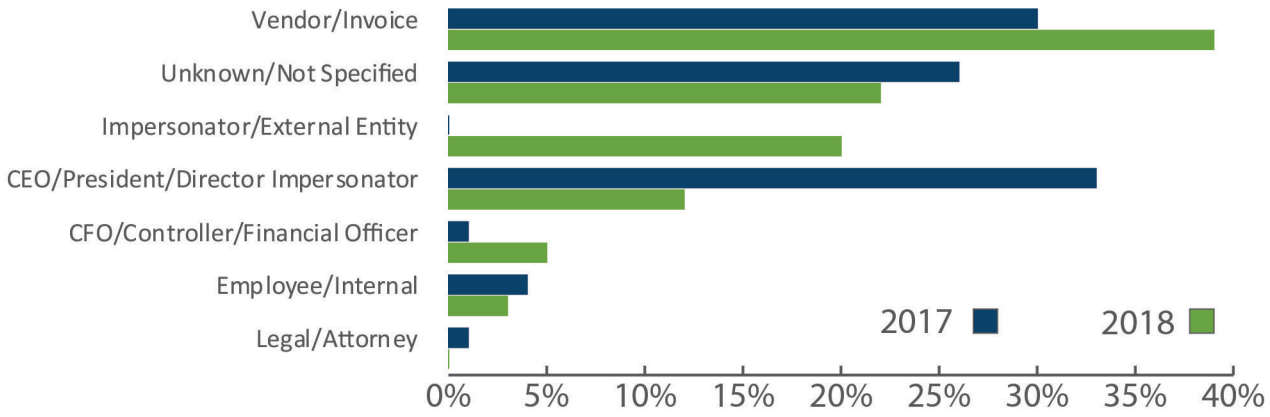
Transactions in 2017 with an initial foreign beneficiary accounted for 27 percent of sampled BEC-related SARs, a decrease from previous years. This decrease may reflect an effort by the perpetrators to reduce the chance of conducting activity appearing out of pattern for victim accounts, in which funds are usually sent domestically, or successes in disrupting international BEC transfers, such as through FinCEN's Rapid Response Program (discussed further below).

Fraudulent Vendor Invoices are Top BEC Methodology

Trends in scam typology indicate that BEC actors are likely changing methods as awareness of their schemes evolves, and new scams emerge. The most frequently used BEC methodology in our 2017 sample involved fraudulent emails impersonating the CEO or president of a company (33 percent), but it declined to 12 percent in 2018, likely due to awareness of such schemes in the business community. Fraudulent vendor or client invoices were 30 percent of incidents in 2017, and grew to 39 percent in 2018, becoming the most common BEC method.

- FinCEN started tracking impersonation of individuals outside the organization in 2018, to account for a shift in scam methods. In 2018, this type of activity accounted for 20 percent of BEC transactions. The vast majority of these SARs reported that the scammer was impersonating a realtor or agent on the sale side of a real estate transaction, directing the buyer or buyer's representatives to wire money to a fraudulent account.
- BEC perpetrators likely impersonate CEOs and CFOs to decrease the likelihood that the wire instructions will be challenged. Financial firms had the highest proportion of transactions involving CEO-impersonation in 2017, representing 14 percent of all BEC transactions analyzed, but accounting for 22 percent of all CEO-related fraud. Perpetrators of BEC fraud targeting financial institutions impersonated the CEO or president in 50 percent of all analyzed transactions.
- Potential for greater financial gain has likely led perpetrators of BEC fraud to use fraudulent vendor invoices when targeting certain industries. The average transaction amount for BECs impersonating a vendor or client invoice was $125,439, compared with $50,373 for impersonating a CEO. Despite representing 30 percent of total transactions, BEC fraud using a fraudulent vendor invoice accounted for 41 percent of total transaction amounts, ranking the highest among the scam typologies observed. For example, an individual in Lithuania was arrested for allegedly using this type of scam to defraud multinational companies, causing them to wire at least $100 million to overseas bank accounts under his control.
- BEC involving fraudulent vendor or client invoices uses an initial foreign counterparty for money laundering more frequently than other methods, likely because of the number of vendors located overseas and the lower probability of the transfer being flagged as fraudulent. Perpetrators of BEC fraud impersonating a vendor or client accounted for 34 percent of all transactions with an initial foreign intermediary in 2017.

Figure 4. 2017 and 2018 BEC Identified Scam Types



FinCEN Rapid Response Program

BEC continues to be an attractive crime for criminal groups because of the high profits and low cost and risk for the perpetrators. The ability to freeze and recover stolen funds has been one method of decreasing its attractiveness to criminal groups. FinCEN's Rapid Response Program is one means to recover stolen funds. Since the inception of the program in 2014, over $500 million has been recovered. There may also be opportunities to improve private sector collaboration in detecting and disrupting these threats, especially during domestic transfers through money mule accounts. Key considerations include how to enable public-private partnerships and rapid sharing of information. FinCEN will continue to monitor BEC trends and will work with law enforcement and other partner agencies to identify methodologies and opportunities to disrupt BEC networks.

FINCEN RAPID RESPONSE PROGRAM

FinCEN's Rapid Response Program (RRP) is a multi-agency and private sector effort to interdict cybercrime-enabled wire fraud. The program leverages relationships with government, financial institution, and law enforcement partners to interdict cybercrime-enabled wire fraud proceeds nationally and globally to return the funds to victims. Under the program, when United States law enforcement receives a BEC complaint from a victim or a financial institution, the relevant information is forwarded to FinCEN, which moves quickly to track and recover the funds. The program utilizes FinCEN's ability to rapidly share information with counterpart Financial Intelligence Units (FIU) in more than 164 jurisdictions, and leverages these relationships to encourage foreign authorities to intercede and hold funds or reverse wire transfers. For more information about the program, contact RRPinfo@fincen.gov.

Disclaimer of Warranties and Endorsement: The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.