FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Business Email Compromise in the Real Estate Sector: Threat Pattern and Trend Information, January 2020 to December 2021

Business Email Compromise in the Real Estate Sector: Threat Pattern and Trend Information, January 2020 to December 2021

Executive Summary: This Financial Trend Analysis provides threat pattern and trend information on Business Email Compromise (BEC) incidents in the real estate sector, based on Bank Secrecy Act (BSA) data filed with the Financial Crimes Enforcement Network (FinCEN) between January 2020 and December 2021 (the Review Period).[1] The perpetrators of these attacks typically aim to defraud individuals and entities in connection with real estate transactions; their techniques include obtaining unauthorized access to networks and systems to misappropriate confidential and proprietary information. Individual homebuyers suffer disproportionately from these incidents. The sector remains a target for BEC attacks exploiting the high monetary values generally associated with real estate transactions and the various communications between entities involved in the real estate closing process.

FinCEN's analysis of BEC incidents specific to the real estate sector (RE-BEC) in information filed with FinCEN pursuant to the BSA (BSA data) during the Review Period indicates that incidents consistently impacted the public. For example:

- *FinCEN identified RE-BEC money laundering typologies*: FinCEN identified money laundering typologies used by RE-BEC attackers, including the use of "money mules," romance scams[2] to recruit unwitting money mules,[3] ties to other fraud types, and use of alternative payment systems such as convertible virtual currency (CVC). Of the 2,013 RE-BEC incidents reported to FinCEN during the Review Period, 4.12% (or 83 incidents) involved CVC such as Bitcoin.
- *Average monthly value of RE-BEC incidents increased, calendar year 2020 versus 2021*: BSA data for 2020 indicates that the average monthly value of RE-BEC incidents was $354,402, with a median value of $108,712. BSA data for 2021 suggests that the average monthly value of RE-BEC incidents was $503,436, with a median value of $131,917. The average total monthly value of RE-BEC incidents in the Review Period was $412,921, with a median value of $116,233 (see Figure 1).

1. The data in this report consists of information filed with FinCEN pursuant to the BSA, herein referred to as "BSA data," and is not a complete representation of all BEC incidents in the real estate sector during the review period. Trends represented in this report illustrate identification and reporting of BEC attacks and may not reflect the dates actually associated with incidents.
2. Romance scams (also referred to as "online dating," "confidence," or "sweetheart" scams) involve fraudsters creating a fictitious profile on an online dating app or website to establish a close or romantic relationship with older adults to exploit their confidence and trust. For more information, see "Advisory on Elder Financial Exploitation," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A002, 15 June 2022, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.
3. Money mules are individuals who transfer money on behalf of BEC perpetrators. These individuals may be witting or unwitting participants in laundering BEC proceeds. Money mules are often recruited online through other scams. For more information, see "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID 19)," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2020-A003, 7 July 2020, https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

- *Title and closing entities most commonly impersonated by RE-BEC attackers*: Actors perpetrate RE-BEC attacks by impersonating authorized persons or entities. The most common victims of impersonation were individuals and entities involved in the title and closing processes within a real estate transaction. For example, of the 2,013 RE-BEC incidents during the Review Period, 37% (or 743 incidents) involved impersonation of title and closing entities (see Figures 2, 3, and 4).
- *Domestic transfers top destination of funds tied to RE-BEC incidents*: Nearly 88% of all RE-BEC incidents during the Review Period – a total of 1,767 incidents – involved initial domestic transfers of fraudulent funds to accounts at U.S. depository institutions. Less than 8% of all RE-BEC incidents, or 151 incidents, involved initial transfers of fraudulent funds to international jurisdictions.[4] Of those 8%, the top international destinations for those funds included the Hong Kong Special Administrative Region of the People's Republic of China (Hong Kong) (18.54% or 28 incidents), followed by Mainland China (China) and Mexico (12.58% or 19 incidents each), Nigeria (9.27% or 14 incidents), and the United Kingdom (7.28% or 11 incidents) (see Figure 5).
- *Mixed success in the recovery of funds by financial institutions*: Of the 2,013 RE-BEC incidents reported to FinCEN during the Review Period, details regarding fund recoveries were unclear or not provided in 30.45% of incidents (or 613 incidents). Of the remaining 69.55% of incidents where recovery data was provided on RE-BEC incidents within the Review Period, filers reported: full fund recoveries for 22.21% (or 447 of incidents); partial fund recoveries for 14.51% (or 292 of incidents); and no fund recoveries for 20.37% (or 410 of incidents). Institutions blocked or declined to process in 12.47% (or 251 of incidents) (see Figure 6).

This Financial Trend Analysis focuses on pattern and trend information identified in BSA data relating to BEC in the real estate sector in 2020 and 2021. This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 (AMLA), which requires FinCEN to periodically publish threat pattern and trend information derived from BSA filings.[5] FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) policy on 30 June 2021, which included cybercrime as a government-wide priority. FinCEN determined that BEC and email account compromise incidents are a cybercrime concern and issued an updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes, FIN-2019-A005, on 16 July 2019 (July 2019 BEC Advisory). The information contained in this report is relevant to the public, particularly individual homebuyers and the multiple entities involved in real estate transactions. The report also highlights the value of BSA information filed by regulated financial institutions, including responses to the July 2019 BEC Advisory.[6]

4. Some RE-BEC filings reported multiple countries in relation to a single RE-BEC incident, resulting in 167 international transfers reported in 151 RE-BEC incidents. Percentages for the top international locations are based on the 167 international transfers.
5. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
6. For more information, see "Advisory to Financial Institutions on Email Compromise Fraud Schemes," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2016-A003, 6 September 2016, https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

Scope and Methodology: FinCEN examined RE-BEC BSA filings between 1 January 2020 and 31 December 2021 to determine trends. The full data set consisted of 2,260 filings during this time period reporting roughly $893 million in RE-BEC incidents.[7] [8] These reports may refer to incidents that occurred in previous months and years. Of the 2,260 RE-BEC filings reviewed, 1,261 were filed in 2020 and 999 were filed in 2021. For the purpose of analysis, FinCEN further subdivided BSA filings by incident date as a subset of the full dataset.

Incident date data: The incident date data set is a subset of the filing date data set that consists of the BSA filings which both (i) reported RE-BEC activities that occurred during the Review Period, and (ii) were filed during the Review Period. Of the 2,260 total filings reviewed, 2,013 report actual incidents that occurred during the Review Period worth $710 million.[9]

FinCEN compared RE-BEC data gathered for the whole of 2020 and 2021 to BSA data gathered on BEC during the Review Period in order to compare trends. This data set consisted of 31,695 BSA filings reflecting roughly $10.8 billion, which both (i) reported BEC activities that occurred during the Review Period and (ii) were filed during the Review Period. Of the 31,695 BEC filings, 16,401 were filed in 2020 and 15,294 were filed in 2021.[10]

What is Business Email Compromise?

BEC is a scam that targets businesses (as well as educational institutions, government, and non-profits) and the financial institutions that transfer their funds. Scammers target organizations that routinely conduct large wire transfers and rely on email for communication regarding the wires. 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.[11] Often, the victim is tricked into thinking a legitimate email from a trusted person or entity is directing them to make a payment. According to the Federal Bureau of Investigation's (FBI) Internet Crime Compliant Center (IC3), BEC incidents resulted in over $43 billion in worldwide losses between June 2016 and December 2021.[12] FinCEN highlighted patterns and red flags associated with BEC, including RE-BEC in particular, in the July 2019 BEC Advisory.[13]

7. FinCEN assessed filings between 1 January 2020 and 31 December 2021 for accuracy, duplication, and false positives using both the narrative and the note to FinCEN field on BSA forms.
8. For the purposes of this report, filings pertaining to December 2021 incidents that were submitted after the Review Period were omitted.
9. Amounts associated with RE-BEC-related incidents may include processed transactions, attempted transactions, and transactions associated with the RE-BEC proceeds.
10. Large suspicious activity filings for attempted, vice actual, BEC incidents were removed from this dataset.
11. For more information, see "Advisory to Financial Institutions on Email Compromise Fraud Schemes," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2016-A003, 6 September 2016, https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.
12. For more information, see "Public Service Announcement: Business Email Compromise The $43 Billion Scam," Federal Bureau of Investigation, 4 May 2022, https://www.ic3.gov/Media/Y2022/PSA220504.
13. For more information, see "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2019-A005, 16 July 2019, https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf.

RE-BEC Money Laundering Typologies

FinCEN identified at least four money laundering typologies attributed to RE-BEC attackers in 2020 and 2021 by analyzing BSA data and leveraging law enforcement observations.

Money Mules Used to Obfuscate Ties to RE-BEC Attackers

First, FinCEN often observed money mules involved in movement of funds following RE-BEC incidents, especially in SAR filings related to accounts to which victim funds were moved. In July 2020, FinCEN issued an advisory to alert financial institutions to potential indicators of money mule schemes tied to multiple fraud typologies.[14] In December 2021, the FBI's IC3 issued a money mule public service announcement, reporting that IC3 had received an increase in complaints regarding fraud and online scams, including BEC.[15] The FBI's public service announcement is part of a larger government effort, known as the Money Mule Initiative, to educate the public about money mules and to disrupt fraud schemes that rely on money mule networks.[16]

Unwitting Money Mules Recruited Through Romance Scams

The second typology FinCEN identified was that RE-BEC fraudsters used romance scams to recruit money mules to receive, and then deplete, funds. Of the 2,013 RE-BEC incidents reported between January 2020 and December 2021, 4.32% (or 87 incidents) referenced a romance scam. Fraudsters used social media platforms and dating sites and applications to cultivate money mules.[17] In addition, 11 filings reported the possibility that a romance scam victim was also a victim of elder exploitation or abuse.[18]

14. For more information, see "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID 19)," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2020-A003, 7 July 2020, https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.
15. For more information, see "Public Service Announcement: Money Mules: A Financial Crisis," Federal Bureau of Investigation, 3 December 2021, https://www.ic3.gov/Media/Y2021/PSA211203.
16. For more information, see "U.S. Law Enforcement Targets Fraud Facilitators, Doubling Last Year's Enforcement: Agencies Increase Awareness About How Fraudsters Use and Recruit Money Mules," U.S. Department of Justice, 3 December 2021, https://www.justice.gov/opa/pr/us-law-enforcement-targets-fraud-facilitators-doubling-last-year-s-enforcement.
17. In some cases, the romance scam victims stated that they had been in contact with the pertinent fraudster(s) for almost a year at the time of the RE-BEC fraud. Romance scam victims frequently referred to the fraudster using romantic terminology (e.g., boyfriend, girlfriend, fiancé, etc.) when speaking to depository institution staff and law enforcement, indicating the extent to which the victims perceived the scam as a real romantic relationship.
18. The actual number of elder exploitation or abuse cases is likely to be higher and not necessarily connected to romance scams. RE-BEC filings frequently did not provide—and their filers might not have had access to—information regarding the ages of romance scam victims and/or money mules.

To receive funds, fraudsters instructed romance scam victims to open a new account (in most cases) at a depository institution and to then transmit that account information back to the fraudsters. Some romance scam victims used their own personal accounts to receive the funds; while others provided the fraudster with their online banking credentials to allow the fraudsters direct access to their account. The fraudsters then used the accounts of the romance scam victims to receive funds from the RE-BEC fraud victim. The instructions that RE-BEC victims received, that resulted in the depletion of their funds, varied among filings. Examples of these instructions included: withdrawing cash from ATMs; wiring funds to another account; and purchasing cashier's checks, gift cards, or CVC.

Accounts Tied to RE-BEC Also Used to Conduct Multiple Fraud Types

An analysis of the accounts involved in RE-BEC incidents, during the Review Period, indicates that fraudsters may be engaged in multiple types of fraud and using the same accounts to receive funds from these acts as the accounts used to receive funds from RE-BEC scams. The analysis indicates involvement in identity fraud, BEC attacks on industries other than real-estate, and other forms of cybercrimes committed by the RE-BEC perpetrators.

FinCEN also observed fraudulent unemployment assistance funds transferring to accounts that were associated with RE-BEC incidents. Of the 2,013 RE-BEC incidents reviewed for this report, 6.81% (or 137 incidents) also involved COVID-19 fraud, with a few instances of multiple types of COVID-19 fraud. Other types of COVID-19 fraud included: economic injury disaster loans fraud; CARES Act Paycheck Protection Program loan fraud; and stimulus payment fraud.

Use of Alternative Payment Methods to Convert Illicit Proceeds

In several RE-BEC incidents, illicit funds quickly moved from bank accounts to online payment platforms, or were used to purchase CVC, most commonly in the form of Bitcoin. Fraudsters generally used CVC exchanges after obtaining RE-BEC proceeds and sometimes instructed money mules to buy CVC at U.S. and international cryptocurrency exchanges. In April 2021, the FBI released a public service announcement annotating a rise in BEC complaints, where victim funds were used to purchase CVCs.[19] FinCEN's analysis of BSA data further confirms this trend. Of the 2,013 RE-BEC incidents, 4.12% (or 83 incidents) involved CVC.

Average Value of RE-BEC Incidents Rises

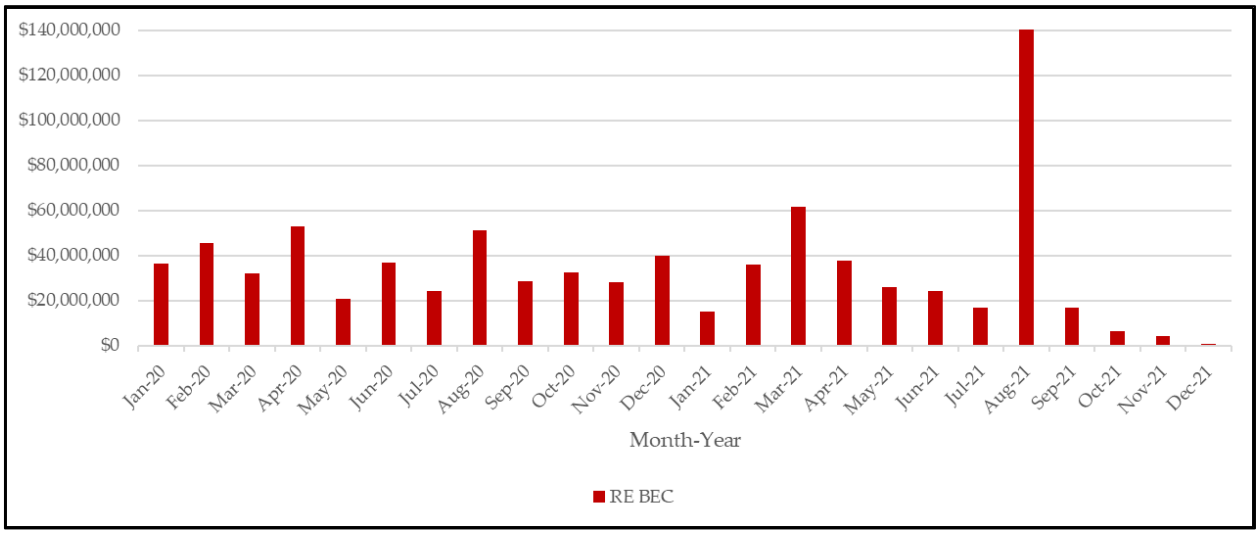
The average value of RE-BEC incidents reported to FinCEN rose in 2021. In 2020, the average monthly value of RE-BEC incidents was $354,402, with a median value of $108,712. In 2021, the average monthly value of RE-BEC incidents was $503,436, with a median value of $131,917. The average total monthly value of RE-BEC incidents in the Review Period was $412,921, with a mean

19. For more information, see "Public Service Announcement: Rise In Use of Cryptocurrency In Business Email Compromise Schemes," Federal Bureau of Investigation, 13 April 2021, https://www.ic3.gov/Media/Y2021/PSA210413.

value of $116,233. This increase could be reflective of trends in home prices between 2020 and 2021. According to the National Association of Realtors, median home sales in 2021 increased 16.9% from 2020, representing the highest on record since 1999.[20]

RE-BEC remained a consistent subset of overall BEC filings received by FinCEN for 2020-2021. RE-BEC incidents as a percentage of overall BEC incidents ranged from 6.02% to 8.13% per month in 2020 and 3.65% to 7.82% per month in 2021. FinCEN previously reported in a July 2019 Financial Trend Analysis report that real estate was the third most targeted sector for BEC fraud in 2017 and 2018, comprising 9% in 2017 and 16% in 2018, respectively, of all industries targeted by BEC attacks in BSA data.[21] FinCEN could not determine what impact COVID-19 disruption, real estate market trends, industry-driven campaigns to prevent RE-BEC, and potential under reporting had on the quantity and quality of reporting for RE-BEC events in the Review Period.[22]

Figure 1. Monthly Suspicious Activity Amounts from RE-BEC by Incident Date, January 2020 to December 2021[23] [24] [25]

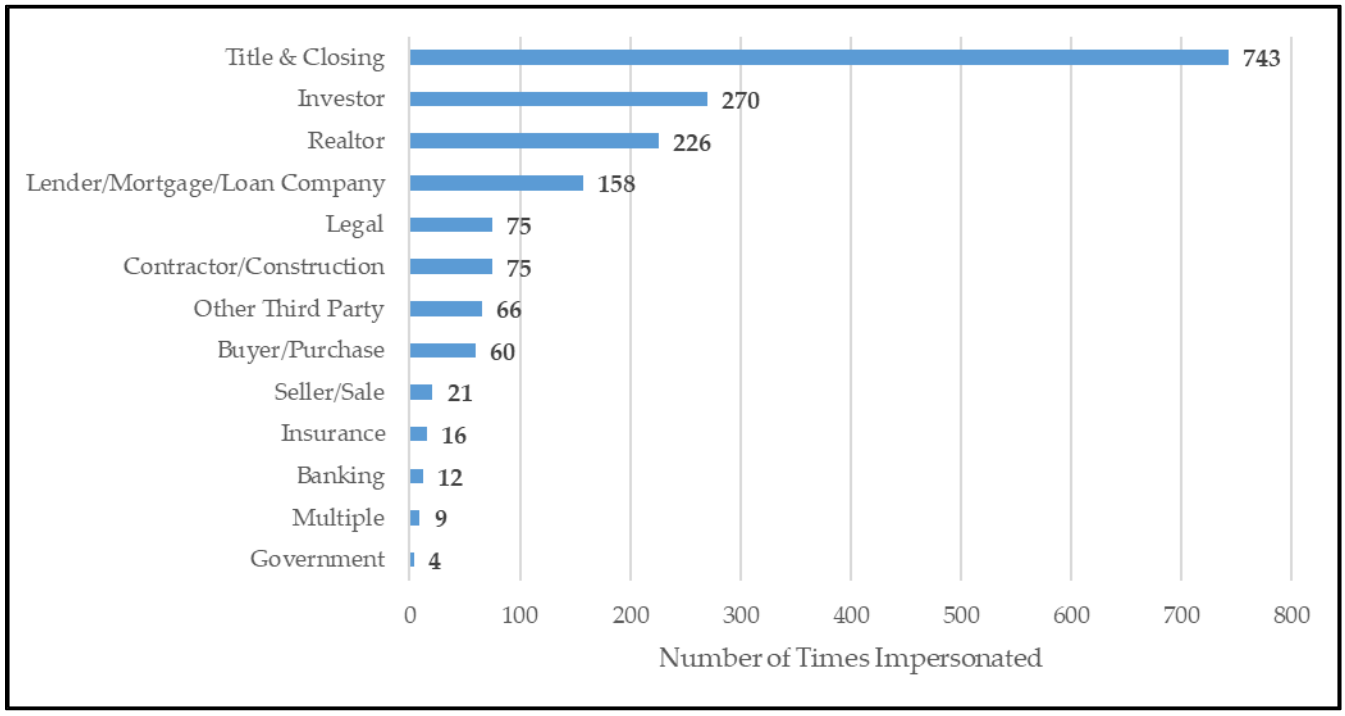


20. For more information, see "Existing Home Sales," National Association of Realtors, https://www.nar.realtor/research-and-statistics/housing-statistics/existing-home-sales.
21. For more information see "Financial Trend Analysis: Manufacturing and Construction Top Targets for Business Email Compromise," Financial Crimes Enforcement Network, July 2019, https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf.
22. For example, see "Coalition to Stop Real Estate Wire Fraud," https://stopwirefraud.org/.
23. Figure 1 is based on transaction date ranges provided by filers in 2,013 filings for the Review Period. Transaction date(s) pertains to the actual date(s) of compromise and fraud. Filers have 30 days to submit a suspicious activity report following the detection of an incident, and in some cases, filings may reference earlier date ranges than their date of submission. FinCEN did not analyze filings submitted after December 2021 for this report.
24. Reporting for the fourth quarter of 2021 may be higher. Data does not reflect submissions that were submitted outside the Review Period for incidents that occurred in the Review Period.
25. Values for August 2021 reflect two attempted transactions totaling $111 million.

Title and Closing Entities Most Frequently Impersonated

Title and closing entities were most commonly impersonated in RE-BEC incidents throughout the Review Period, though they may not have been the ultimate victim of financial loss.[26] Of the 2,013 incidents, 36.91% (or 743 incidents) involved the impersonation of a title or closing company (see Figure 2).

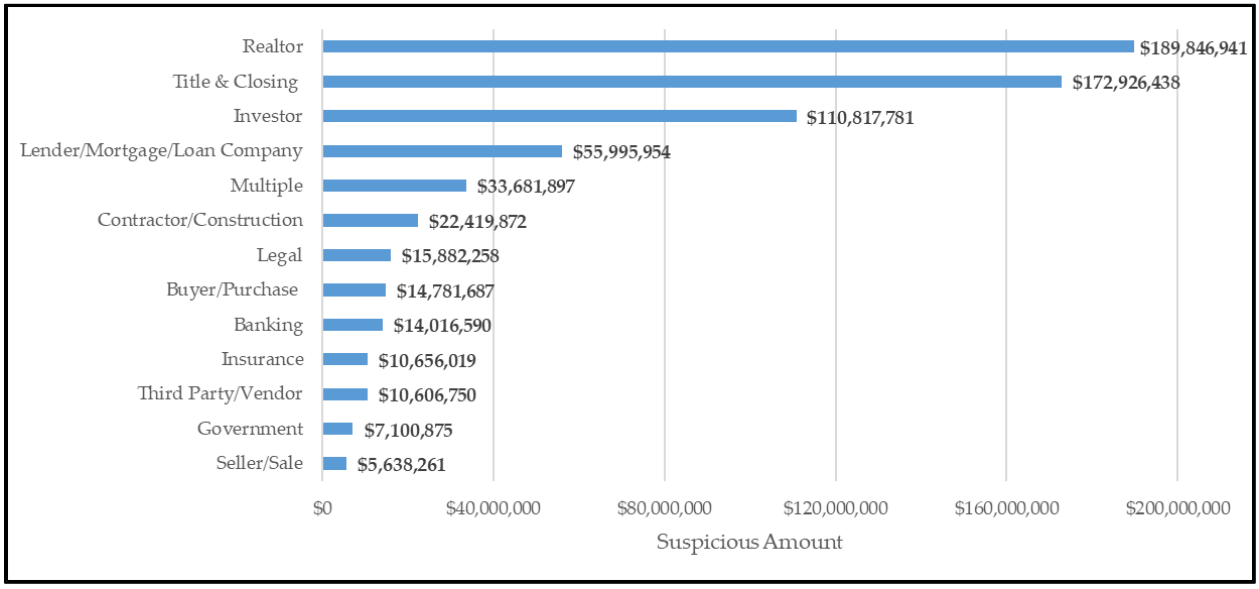
Figure 2: Impersonated Parties in RE-BEC BSA Filings,
January 2020 to December 2021



Realtor impersonations comprised 23.12% (or $189.8 million) of the overall values in suspicious RE-BEC activity reported during the Review Period, only slightly ahead of title & closing entities at 21.06% (or $172.9 million), followed by investors representing 15.6% (or $110.8 million) of suspicious activity (see Figure 3).[27]

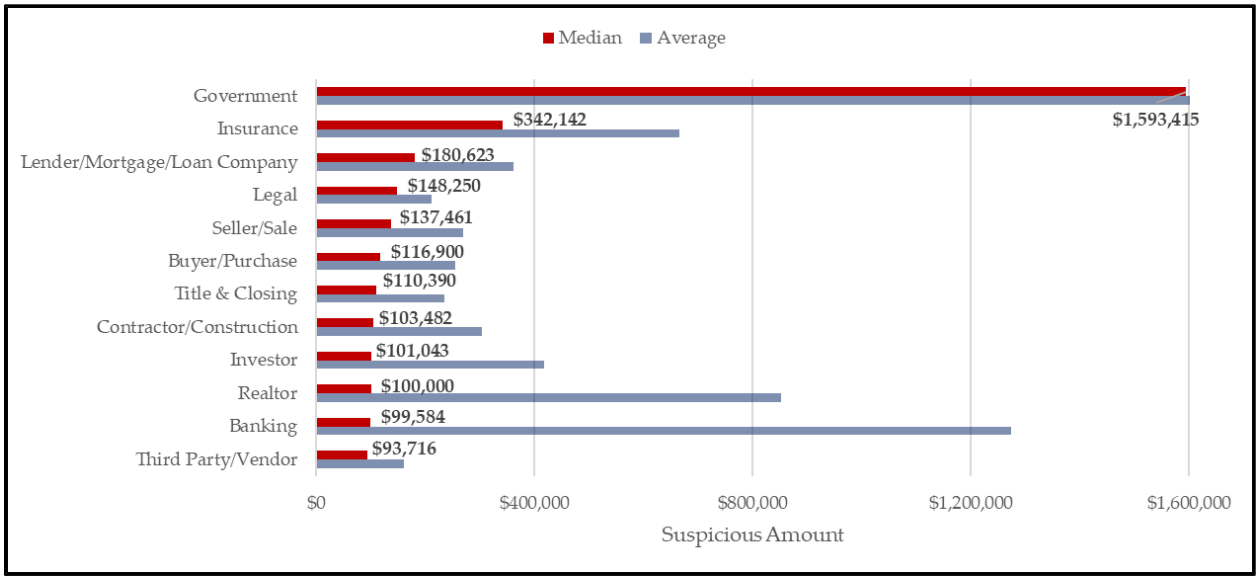
26. An entity does not necessarily suffer financial losses merely because it was impersonated in connection with an RE-BEC attack. Fraudsters may impersonate one party to a real estate transaction, such as an investor, to defraud another party to the transaction, such as a purchaser.
27. Investors are buyers in real estate transactions that purchase property as an investment.

Figure 3. Value of Suspicious Activity by Impersonated Party, January 2020 to December 2021[28]



Although fraudsters tended to impersonate title and closing entities, RE-BEC attacks were most lucrative when fraudsters impersonated government entities, such as federal, state, and municipal agencies (see Figure 4).

Figure 4. Average and Median Suspicious Amount by Impersonated Party, January 2020 to December 2021[29]

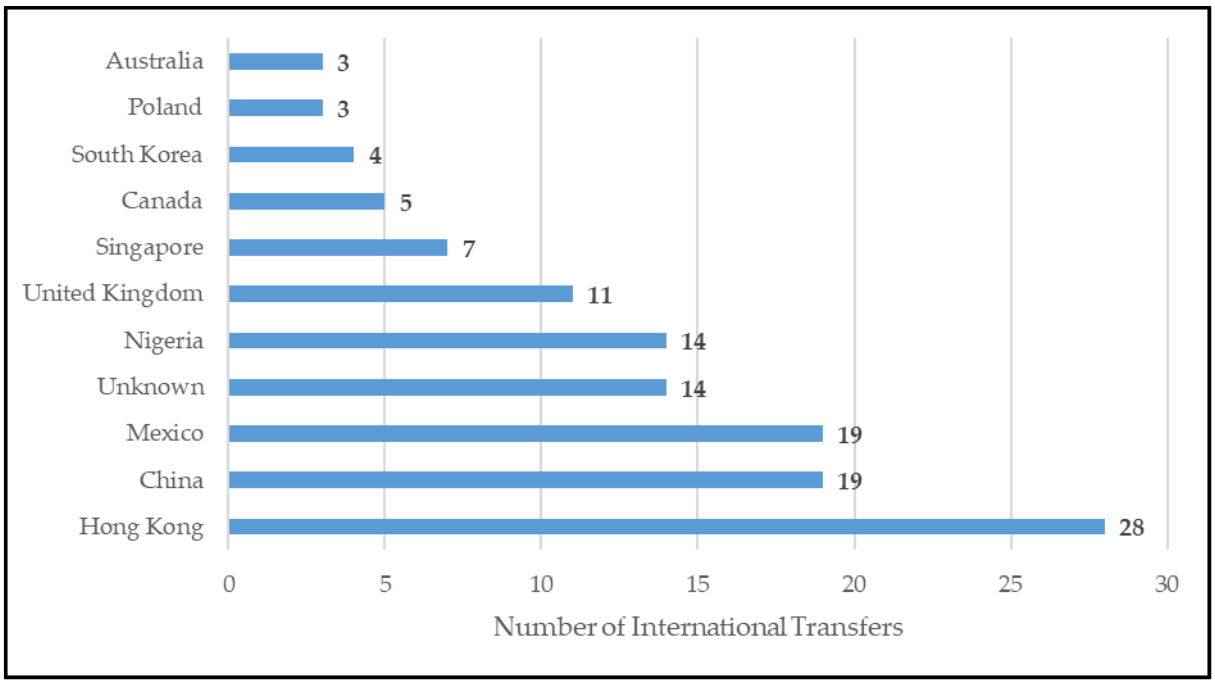


28. Some RE-BEC filings failed to identify the category of victim. The data reported in Figure 3 does not reflect those RE-BEC filings.
29. Median values more accurately reflect the amount of funds stolen per impersonated transaction than average values. Average values include very high and low outliers, which may skew the data, while medians represent the "middle" of data sets.

Domestic Transfers Top Destination of Funds; Hong Kong Top for International Transfers

Nearly 88% of all RE-BEC incidents during the Review Period – a total of 1,767 incidents – involved initial domestic transfers of fraudulent funds to accounts at U.S. depository institutions. Less than 8% of all RE-BEC incidents, or 151 incidents, involved initial transfers of fraudulent funds to international jurisdictions. Of those 8%, the top international destinations for those funds included Hong Kong, Mexico, China, and Nigeria (see Figure 5). Among the 151 incidents reviewed, Hong Kong was the most frequent destination of foreign transfers with 28 incidents (18.54%), followed by China and Mexico at 19 incidents each (12.58% each), Nigeria at 14 incidents (9.27%), and the United Kingdom at 11 incidents (7.28%).

Figure 5. Locations and Frequency of International Transfers, January 2020 to December 2021

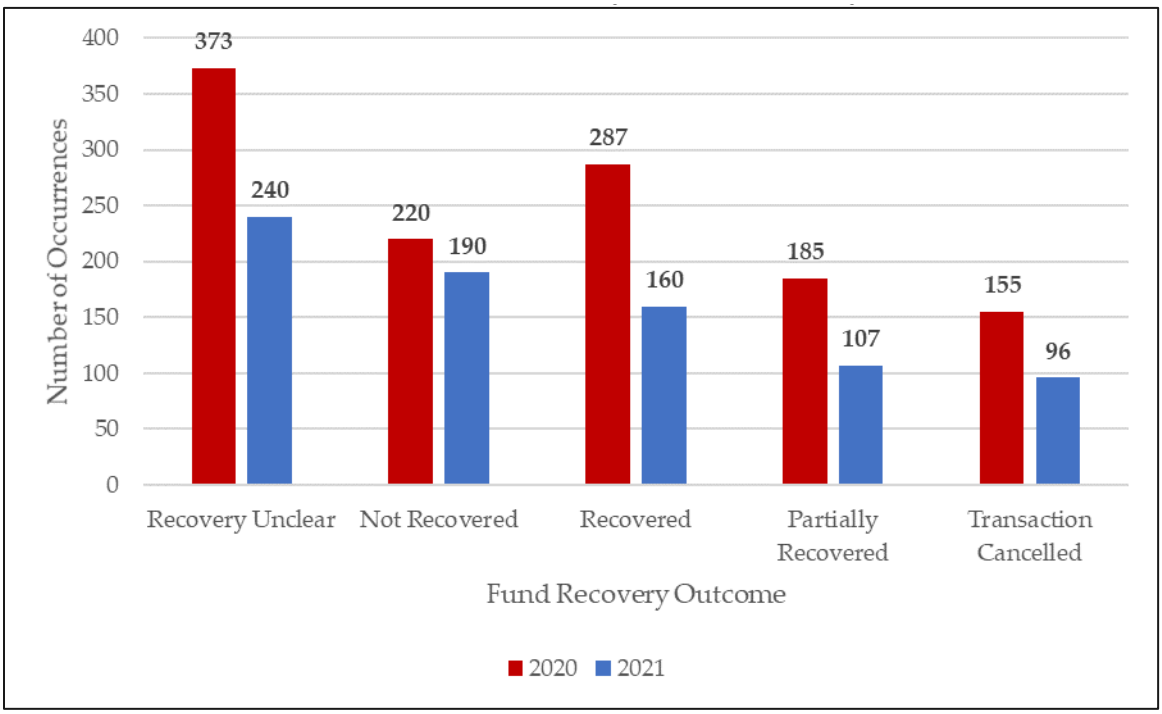


Varying Levels of Success for Recovering Funds among Financial Institutions

Of the 2,013 RE-BEC incidents reported to FinCEN during the Review Period, 30.45% (or 613 incidents) either did not mention fund recovery or were filed shortly after recovery efforts had been initiated. Therefore, final outcomes were unknown. Fund recovery success rates for those cases could not be determined. Of the remaining incidents, there were 22.21% (or 447 incidents) in which depository institutions recovered the full amount of the intercepted funds, 20.37% (or 410 incidents) in which no funds could be recovered, 14.51% (or 292 incidents) in which some funds were recovered, and 12.47% (or 251 incidents) in which the financial institution did not process the

fraudulent transaction.[30] A comparison of fund recovery outcomes in 2020 versus 2021 provides a mixed picture of the trend in successful recovery of funds (see Figure 6). For example, funds not recovered increased from 18.03% in 2020 to 23.96% in 2021. Recovered funds reported fell from 23.52% in 2020 to 20.18% in 2021. Fund recovery is especially important in the aftermath of RE-BEC incidents, as many victims are individual homebuyers who may face significant financial hardship due to the loss of funds.[31]

Figure 6. Outcomes of RE-BEC Fund Recovery Efforts, January 2020 to December 2021



RE-BEC Detection, Mitigation, Prevention, and Reporting

Financial institutions, entities within the real estate sector, and the general public may all play an important role in protecting the U.S. financial system from RE-BEC attacks through awareness of actions to detect and mitigate attacks, information sharing mechanisms that can prevent attacks, and various ways to report incidents when they occur.

30. Many of the filings did not indicate whether fund recovery efforts were attempted. Furthermore, among the filings that stated that fund recovery efforts had been attempted, not all of them provided how much, if any, had been recovered.
31. *See* section below on "RE-BEC Detection, Mitigation, Prevention, and Reporting" for more information on how to recover funds.

Detection and Mitigation

FinCEN encourages the following actions for financial institutions, entities within the real estate sector, and the general public to detect and mitigate RE-BEC and other types of BEC incidents:

1. Assess the vulnerability of their business processes with respect to BEC and, consider actions to "harden" or increase the resiliency of their processes and systems against email fraud schemes. The scale of actions in this latter category would correlate to quantifiable risk associated with three common practices: (1) authentication of participants involved in communications; (2) authorization of transactions; and (3) communication of information and changes about transactions.

2. Adopt a multi-faceted transaction verification process—as well as training and awareness-building—to identify and evade spear phishing attempts. For instance, financial institutions should verify the authenticity of suspicious transaction payment instructions sent via email by using multiple means of communication, or by contacting others authorized to conduct the transactions. Identifying fraudulent transaction payment instructions before payments are issued is essential to preventing and reducing unauthorized transactions.

FinCEN also promotes awareness of the critical role of timely reporting and activating the Rapid Response Program (RRP) in an effort to interdict, freeze, and recover funds stolen by cyber-enabled fraud, such as BEC. FinCEN administers the RRP in partnership with the FBI, the U.S. Secret Service (USSS), Homeland Security Investigations (HSI), and the U.S. Postal Inspection Service and counterpart foreign Financial Intelligence Units. The program leverages relationships with government, financial institution, and law enforcement partners to interdict cyber-enabled wire fraud proceeds globally and then return the funds to victims. In FY 22, FinCEN acted on 806 referrals concerning wire transfers collectively valued at more than $356 million of allegedly fraudulently stolen funds. FinCEN and its partners froze approximately $174 million for further investigation and potential return to victims, which is approximately 49% of the reported funds stolen in FY22. Since the inception of the RRP in 2014, the program has aided in the identification and freezing of more than $1.3 billion for U.S. victims of fraud, which is a total success rate of 51%. While the recovery of BEC stolen funds is not assured, FinCEN has had greater success in identifying and freezing funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 72 hours of the transaction. Financial institutions should be prepared to provide transactional details and cyber-related information surrounding the cyber-enabled financial fraud incident, such as BEC, when requesting assistance in recovering funds.[32]

32. For more information see "Fact Sheet on the Rapid Response Program (RRP)," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-FCT1, 11 February 2022, https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf.

Prevention through Information Sharing

Due to the nature of BEC incidents overall, FinCEN encourages communication among financial institutions under the auspices of section 314(b) of the USA PATRIOT Act, which permits the reporting of activities that they suspect may involve possible terrorist activity or money laundering. Sharing of such information could also help prevent billions of dollars in potential losses to financial institutions and their customers.[33]

Reporting Cyber-Enabled Crimes

Financial institutions play an important role in protecting the U.S. financial system from RE-BEC attacks through compliance with BSA requirements. Financial institutions should determine if a suspicious activity report filing is required or appropriate when dealing with a RE-BEC incident.[34] As a reminder, a financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[35] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[36] Financial institutions may also file with FinCEN a report of any suspicious transaction they believe relates to the possible violation of any law or regulation but whose reporting is not required by 31 CFR Chapter X.

To report business email compromise, contact the FBI's IC3 www.ic3.gov or contact the nearest USSS field office through http://www.secretservice.gov/field_offices.shtml. Contact OFAC at ofac_feedback@treasury.gov if there is any reason to suspect the cyber actor may be sanctioned or otherwise have a sanctions nexus.

The information in this report is based on BEC-related information obtained from analysis of BSA data, trade publications, and commercial reporting, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.

33. For more information see "Section 314(b) Fact Sheet," Financial Crimes Enforcement Network, December 2020, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.
34. For more information see "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," Financial Crimes Enforcement Network, FinCEN Advisory FIN-2019-A005, 16 July 2019, https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf.
35. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
36. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.