Federal Bureau of Investigation

Business Email Compromise and Real Estate Wire Fraud

2022

Table of Contents

I. Overview of Reporting Requirement

The Joint Explanatory Statement accompanying the Consolidated Appropriations Act, 2022 (P.L. 117-103) included language directing the Department of Justice to "explore ways to increase collaboration and coordination with industry and other private sector partners, and the FBI is directed to release, within 30 days of the date of enactment of this Act, a public report on the threats from business email compromise (BEC) and related scams."

II. Executive Summary

This report summarizes the primary efforts of the FBI in combatting the BEC threat and its related scams (e.g., email account compromise or EAC) and real estate wire fraud (REWF) by working with domestic and international partners to identify perpetrators and dismantle their organizations.

III. Threat Framework

Overview

BEC is one of the fastest growing, most financially damaging internet-enabled crimes. It is a major threat to the global economy. In 2021, the Internet Crime Complaint Center (IC3) received BEC-related complaints with claimed losses exceeding $2.4 billion.[1] For context, the IC3 found yearly losses attributable to BEC actors were $360 million in calendar year 2016.[2] The sophistication of BEC criminal actors and their ever- evolving tactics has similarly increased over time, likely driving the increased dollar losses. BEC actors have targeted large and small companies and organizations in every U.S. state and more than 150 countries around the world.

The FBI has prioritized mitigating and disrupting the BEC threat, working with domestic and international partners to identify perpetrators and dismantle their organizations.

REWF is a sub-category of BEC, in which criminal actors target individuals or companies executing large wires related to real estate transactions. Often, the criminals pose as parties to the transaction and directly communicate with the other parties to steal funds intended to pay for the real estate. According to IC3 complaint data, victims participating at all levels of a real estate transaction have reported such activity, including title companies, law firms, real estate agents, buyers, and sellers. The FBI has specifically focused on addressing REWF due to its prevalence in the United States and the effect it can have on the individual victims of the REWF schemes, who may be home buyers wiring their life savings. The FBI has prioritized this threat through outreach, education, and training to the real estate and related banking and services industries.

In REWF, the criminal finds a way to insert themselves into a real estate transaction through compromising parties' email or other digital communications. Once the transaction has reached a point where funds begin changing hands, the criminal intervenes and directs the funds to accounts in their control, typically by way of an email that appears to be from the title company, real estate

[1] The 2021 IC3 Annual Report can be found at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] The 2016 IC3 Annual Report can be found at https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf

company, or another interested party. The funds are transferred to the criminal well before the buyer is made aware of the theft. REWF is unique within BEC scams insofar as many times, the buyer is using the proceeds from a home sale to fund a new home purchase, or even the buyer's life savings. The loss of these funds is potentially catastrophic for the victims and their families.

Once taken, the funds are typically directed to a fraudulent domestic account, then quickly dispersed through cash or check withdrawals. As seen in many BEC scams, the funds may be transferred to a secondary fraudulent domestic or international account. Funds sent to domestic accounts are often depleted rapidly, making recovery difficult.

Criminals have been refining their exploitation of technology, especially the internet, to carry out financial crimes. With an increase in internet-enabled financial frauds—such as bank account take-overs, synthetic identity related frauds, money laundering through virtual currency, and BEC—the FBI has pivoted its approach to address this issue through gathering intelligence, utilizing advanced investigative techniques in conjunction with traditional financial crimes investigative techniques, using proactive public and private partnerships, and education and awareness campaigns.

How Criminals Use BEC

BEC scams rely on deception and social engineering to convince victims—including companies, charities, schools, real estate purchasers, and the elderly—to send money, usually via wire transfer, to bank accounts controlled by criminal actors. While there are many variations, BEC schemes often involve the spoofing of a legitimate, known email address or the use of a nearly identical address to appear as someone known to or trusted by the victim. BEC scams are initiated when a victim receives false wire instructions from a criminal attempting to redirect legitimate payments to a bank account controlled by fraudsters; such scams are constantly evolving as criminals become more sophisticated. Over the last several years, the scam has progressed from spoofed emails purportedly from chief executive officers requesting wire payments be sent to fraudulent locations to impersonation of vendor emails; spoofed lawyer email accounts; requests for W-2 information; diversion of payroll funds; the targeting of the real estate sector; and fraudulent requests for large amounts of gift cards.

Following the emergence of COVID-19, BEC actors quickly took advantage of the uncertainty faced by many businesses, often impersonating vendors and requesting payment outside the normal course of business due to the pandemic. The FBI is also aware of multiple incidents in which state government agencies, attempting to procure ventilators or personal protective equipment, wired transferred funds to fraudulent brokers and sellers in advance of receiving the items. The brokers and sellers included both domestic and foreign entities. In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship. By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred to foreign jurisdictions and were unrecoverable by U.S. law enforcement.

The COVID-19 pandemic and the restrictions on in-person meetings led to increases in telework or virtual communication practices. These work and communication practices continued into 2021, and the IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to

request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio or video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions.

How BEC Actors Move Funds

Criminals who obtain money illegally, including through BEC and other fraud, must find a way to move and hide their illicit funds. Money laundering typically involves three stages. First, criminals must "place" the funds into a financial system. The next stage, "layering," involves moving the funds around, often between multiple financial institutions and often between accounts held in false identities or sham companies, to separate the money from its illicit source. The third stage, concealment, helps to conceal the perpetuators of the scheme from detection. The funds are often moved via wire transfer, checks of various kinds, money service businesses (MSBs) such as Western Union and MoneyGram, virtual currency, or combinations of these and other payment methods.

In BEC schemes, criminals frequently rely on third-party facilitators, including money mules, to move these illicit proceeds through funds transfers, physical movement of cash, or other methods. Third party facilitators are those who may or may not be aware of their involvement in these schemes but help to move the funds in such a way to disguise the source of the funds. Those individuals and institutions that help to launder funds knowingly, and typically for a fee, are what the Financial Action Task Force calls professional money launderers.[3] This can include attorneys, accountants, investment managers, and even real estate professionals. Professional money launders can also include individuals who open accounts at financial institutions in the names of synthetic or stolen identities and shell companies for the purpose of concealing the true identities of the criminals who are knowingly receiving and moving the diverted funds.

Money mules may be witting or unwitting and may or may not be aware of the initial source of funds or the funds' unlawful nature. Often, money mules are unaware that they have been taken advantage of themselves. While there are money mules who are aware of their role and move the funds in exchange for a fee, money mules are not typically considered professional money launderers, and criminals frequently leverage the *unwitting* money mules to help move and conceal their illicit proceeds. Unwitting money mules are unaware of their part in a larger scheme and are often victims of online financial, lottery, charitable, or romance fraud schemes; they are asked to use their personal bank account to send or receive money under false pretenses. Money mules primarily facilitate the placement and layering stages of money laundering. However, every money mule adds a layer of obfuscation to the BEC scheme and further complicates the process of getting the stolen money back into the hands of victims, particularly in circumstances when the proceeds are moved to overseas accounts.

[3] The Financial Action Task Force is a global money laundering and terrorist financing watchdog. Founded as an initiative of the G7 in 1989, the Task Force was charged with developing policies to combat money laundering; in 2001, its mandate was expanded to include terrorism financing.

IV. FBI Instruction and Preparation

The FBI utilizes a multi-pronged approach to combat the BEC threat. This includes internal and external awareness campaigns, coordination with domestic and international law enforcement and intelligence partners, and organized takedowns of BEC actors and money mules in the United States and abroad.

The FBI works to proactively address BEC by training the FBI workforce, federal, state, and local law enforcement partners, international partners, and the private sector. In addition, the FBI has committed significant resources to community outreach and education, teaching U.S. citizens about common red flags of BEC schemes and money mule activities and about ways to report suspected instances of BEC fraud.

The FBI provides comprehensive training to FBI agents, analysts, and support staff focused on BEC schemes and money mules. This training is aimed at instructing personnel on the nature and scope of the threats, aiding personnel in identifying these schemes, and highlighting available resources for potentially recovering fraudulently obtained funds as well as charges applicable to this type of activity. The FBI frequently receives requests from domestic and international law enforcement partners for training on both the BEC and money mule threats, and it has designed and delivered numerous training programs.

The FBI has strong relationships with its private sector partners. It has leveraged these relationships to raise awareness of the BEC and money mule threats, and to exchange valuable and timely information related to specific instances of BEC frauds and money mule activity as well as emerging trends, activities, and high-risk jurisdictions related to both.

The FBI frequently provides training to financial institutions, the real estate industry, and technology company representatives on current financial crime trends. These trainings always include information on BEC and money mules, and, like the training provided to FBI personnel, cover common red flags of BEC schemes and money mule activities and ways to report suspected instances of BEC fraud.

During the COVID-19 pandemic, the FBI has organized and delivered training to over 3,000 financial institution representatives, regulators, and business owners on COVID-19-related fraud schemes, including the emerging BEC schemes and increased utilization of money mules. The FBI also leverages its strong relationships with financial institutions in the actions of the IC3's Recovery Asset Team (RAT), which is discussed in greater detail below.

To educate the public on money mules, the FBI has developed a Money Mule Awareness Booklet (Booklet), which provides information on what a money mule is, how money mules are used, indicators that an individual may have been targeted to act as a money mule, and the consequences of undertaking money mule activity. The Money Mule Awareness Booklet is available on FBI.gov and it has been offered to financial institutions to provide to customers they believe may be operating as either witting or unwitting money mules. In addition to the Booklet, the FBI has published multiple Public Service Announcements (PSAs) and has initiated social media campaigns that highlight the threats posed by both BEC schemes and money mules. A recent PSA is included in the Appendix to this report.

The FBI hosts and participates in many national and international conferences that address both BEC and money mules. These conferences include those hosted by regulators, such as the Federal Reserve Board, the National Credit Union Association, and the Federal Deposit Insurance Corporation, as well as those hosted by specialized organizations and industry groups, such as the Association of Certified Anti-Money Laundering Specialists, the International Association of Financial Crimes Investigators, the Mortgage Brokers Association, and the American Bankers Association. Finally, the FBI, at both the national and local level, engages with the media to spotlight BEC schemes and money mules. Lastly, the FBI has done interviews with AARP Magazine, National Public Radio, The Dr. Oz Show, and ABC Nightline.

V. Operations Combatting the Threat

The FBI has numerous initiatives designed to address BEC and the associated money mule threat. These initiatives provide resources that bolster FBI field offices' abilities to address these pressing threats efficiently and effectively. While the BEC and money mule threats are frequently intertwined and often addressed as such, each threat is significant enough to also warrant singularly focused efforts.

Global Takedowns

For the past several years, BEC has consistently been the largest dollar loss by victim crime typology reported to IC3, with over $2.4 billion of adjusted losses in the calendar year 2021. For comparison, the second highest dollar loss category reported to IC3 was investment fraud, with losses of approximately $1.45 billion.[4] In other words, dollar losses associated with BEC were over 65% more than dollar losses associated with investment fraud.

Acknowledging the growing scope of the BEC threat, the FBI has consistently assumed a leadership role in global takedowns aimed at curtailing BEC activity, including Operation Wire Wire, the subsequent Operation reWired, and the recent Operation Eagle Sweep.[5]

Operation reWired

In 2019, the FBI led reWired, a multi-agency, multi-nation effort, to disrupt and dismantle international BEC schemes. Similar to Operation Wire Wire in 2018, reWired surged FBI resources to collectively propel investigative actions against perpetrators of BEC schemes during a focused period both domestically and abroad.

In the United States, reWired focused on arresting, interviewing, and serving Money Mule Warning Letters (MMWLs) on U.S.-based BEC criminals; internationally, the FBI assisted foreign law enforcement with actions on BEC criminals in their countries, actions on criminals in the United States who have victimized foreign citizens, and assisted the Departments of State and Justice with extraditions from foreign countries to the United States, when appropriate. The operation led to

[4] 2021 IC3 Report.
[5] For details, see: https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals

over 280 arrests, including 74 in the United States, 167 in Nigeria, 18 in Turkey, 15 in Ghana, and 7 in France, Italy, Japan, Kenya, and the UK. The operation also resulted in the seizure of nearly $3.7 million, and the disruption and recovery of approximately $118 million in fraudulent wire transfers.

Between August 29, 2019, and September 6, 2019, Nigeria's Economic and Financial Crimes Commission arrested 23 subjects of BEC investigations, including five individuals connected to FBI investigations. Beyond the arrests and seizures, reWired resulted in the establishment of new partnerships in high-risk countries and reinforced existing partnerships.

Operation Eagle Sweep

In 2021 and 2022, the FBI led Operation Eagle Sweep, with the assistance of several agencies and numerous international partners. The operation revealed that BEC scammers were responsible for approximately $51 million in losses and over 500 victims in the United States.

The coordinated effort was significant and disrupted BEC schemes that intercepted and stole wire transfers sent by hundreds of businesses and individuals. The FBI and other U.S. Department of Justice (DOJ) and international law enforcement partners carried out Operation Eagle Sweep over a three-month period and arrested 65 suspects in the United States and overseas, including 12 in Nigeria, eight in South Africa, two in Canada, and one in Cambodia. In parallel with Operation Eagle Sweep, Australia, Japan, and Nigeria conducted local operations targeting BEC actors.

Money Mule Initiative

In December 2021, the DOJ, FBI, U.S. Postal Inspection Service (USPIS) and other federal law enforcement agencies announced the completion of the fourth annual Money Mule Initiative, which targeted networks of individuals through which international fraudsters obtain proceeds of fraud schemes. U.S. law enforcement took action to address 4,750 money mules over the 10 weeks; enforcement actions occurred in every state in the country. These actions more than doubled the number of actions taken during last year's effort when law enforcement acted against over 2,300 money mules. Agencies also conducted outreach to educate the public about how fraudsters use money mules and how to avoid unknowingly assisting fraud by receiving and transferring money. The campaign was conducted simultaneously with a Europol initiative, the European Money Mule Action (EMMA).

The thousands of actions taken by law enforcement ranged from warning letters to civil and administrative actions, to criminal prosecutions. Law enforcement served approximately 4,670 letters warning individuals that their actions were facilitating fraud schemes. These letters outlined the potential consequences for transferring money acquired illegally. Civil or administrative actions were filed against 11 individuals, and through seizures and voluntary return of funds, law enforcement obtained nearly $3.7 million in fraud proceeds.

Concurrent with the completion of this initiative, the FBI released a PSA, which is also included in the Appendix to this report.

Proactive Targeting

The FBI manages an initiative focused on the proactive targeting of high-priority threat actors, including BEC and money mule actors, through the exploitation of Bank Secrecy Act (BSA) data. After the identification of potential targets based on established threat criteria, the BSA data is combined with other FBI and Intelligence Community reporting into a targeting package that is disseminated to the appropriate field office for case initiation.

In 2016, recognizing that over 50% of international wires involving fraudulently obtained funds are destined for Hong Kong and China, the FBI established measures to identify nominee shareholders and directors behind the accounts receiving the illicit funds. This information is shared with appropriate FBI personnel abroad for action deemed appropriate, including information sharing with international partners and affected financial institutions.

Greater awareness of beneficial ownership information allows for field offices, Legal Attaché offices, international partners, and financial institutions to coordinate their efforts and pursue illicit funds more effectively. For example, information received on fraudulent Hong Kong beneficiaries is sent to field offices for further investigation or to victims or their attorneys attempting to retrieve funds by working with financial institutions or the Hong Kong legal system. In addition, field office personnel working on a case or court hearing that references a Hong Kong company suspected of BEC activity can request a search of documents on a specific company from the FBI.

VI. FBI Partnerships

Recognizing the multifaceted and cross-programmatic nature of the BEC and money mule threats, the FBI leverages the capabilities and expertise of various programs within the organization through the internal BEC Working Group (BECWG), which includes representatives from CID, the Cyber Division (CyD), and the IC3. The BECWG has coordinated several large-scale international BEC takedowns from 2018 through 2021. The BECWG shares resources, intelligence, and best practices with international domestic and law enforcement partners and the financial industry.

The FBI works closely with the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) as well as foreign financial intelligence units and banks throughout the world. These relationships have led to the development of various methods to help victims retrieve some or all of their stolen funds. Recognizing that fifty percent of BEC wires stay within the United States before being moved abroad, the FBI launched the IC3 RAT in early 2018. The RAT is designed to assist FBI field offices with the rapid recovery of funds for victims who made transfers to domestic accounts. In 2021, the RAT reported just over 1,700 incidents, with losses approaching $445 million. However, the FBI was able to achieve a success rate near 75%, leading to over $328 million of the $445 million being frozen at recipient financial institutions and made available for recovery.[6]

The FBI shares operational and strategic intelligence related to BEC actors and money mule networks with its foreign partners via several mechanisms. While serving as Chair of the Five Eyes Law Enforcement Group (FELEG) in 2016, the FBI highlighted the global impact of BEC and

[6] The source is the IC3 2021 Report.

money mule networks and worked to identify opportunities for FELEG partners to work together to address these threats.

The FBI also participates in the International Mass-Marketing Fraud Working Group (IMMFWG), which is composed of investigators, enforcers, analysts, prosecutors, and others from member governments and combats fraud involving mass communication (e.g., internet, email, telephone, and postal services). The IMMFWG consists of law enforcement, regulatory, and consumer protection agencies from Europol, Belgium, Canada, Netherlands, Nigeria, Spain, the UK, and the United States. It has been an effective method for the sharing of best practices and approaches for addressing BEC and money mule threats. The IMMFWG is a collaborative resource that meets on a regular basis to exchange intelligence; coordinate cross-border operations to disrupt and apprehend mass-marketing fraudsters; develop strategic projects; and discuss awareness, education, and prevention campaigns for the public. U.S. agencies that participate in the IMMFWG include the DOJ Consumer Protection Branch, the Federal Trade Commission, Homeland Security Investigations, Internal Revenue Service Criminal Investigation (IRS-CI), and U.S. Secret Service (USSS).

The FBI has 63 Legal Attaché offices and dozens of sub-offices located in key cities across the globe, providing coverage for more than 180 countries, territories, and islands. Each office is established through mutual agreement with the host country or territory, and is situated in the U.S. embassy or consulate in that location. Recent global initiatives have led to stronger relationships and the establishment of working groups in high-risk jurisdictions that have been successful in combating the threat. The FBI is also working internally and with other federal agencies to build a footprint in areas where BEC is not sufficiently addressed.

As noted above, multiple federal agencies assist in countering the BEC threat. Responsibilities vary depending on their respective mandates and statutory guidelines and responsibilities. For example, in some cases, the IRS-CI is the best possible partner due to the tax implications of a particular matter; in other cases, the USPIS is the best possible partner given their responsibilities with the U.S. mail service. The FBI uses its extensive domestic and international connections to work these matters, coordinating and deconflicting investigations across the United States and the world.

The FBI has been the lead federal agency on matters related to BEC since it began specifically tracking BEC complaints received by IC3 in 2013. Since that time, the FBI has involved and aided other federal agencies in BEC-specific operations, such as those referenced above. The extensive knowledge and network of partners around the globe allow the U.S. Government to aid in returning the proceeds of BEC schemes to their rightful owners.

VII. Information Gaps and Recommendation

The FBI has identified vulnerabilities which, if addressed, would bolster the ability of U.S. law enforcement to effectively address a wide range of threats, including BEC and money mules.

Beneficial Ownership Information Critical

The illicit proceeds gained through BEC and other fraud schemes are frequently moved through and end up in accounts controlled by shell or front companies. The Corporate Transparency Act (CTA) provides for the creation of a national, non-public database of underlying beneficial ownership information for U.S.-registered businesses that meet specific criteria.[7] The data collected will be made available to U.S. law enforcement, subject to certain guardrails, offering a critical resource for identifying participants in a BEC scheme.

On September 29, 2022, the Financial Crimes Enforcement Network (FinCEN) issued the first of three rulemakings to implement the CTA. This first rulemaking governs who must report and what information they must report to FinCEN; the final rule will take effect on January 1, 2024. FinCEN is working to implement the database to house this information; therefore, its efficacy as a tool to counter BEC activity has yet to be measured. Moreover, the CTA exempts from its reporting requirements various types of entities, including trusts, which may affect efforts to identify the beneficial owners of trusts or other entities engaged in REWF.

Uniform Commercial Code Issue

Uniform Commercial Code (UCC) 4A-207 Mis-Description of Beneficiary states if the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the number as the proper identification of the beneficiary of the order. The beneficiary's bank does not need to determine whether the name and number refer to the same person. When BEC acts occur, the bank does not have to verify the transfer beyond the number. In order to address this shortcoming, it is recommended that UCC 4A-207 be redrafted to require banks to properly identify the name and number of the beneficiary and to determine they are in fact the same individual or entity.

VIII. Conclusion

The FBI has led the charge against BEC and money mule threat actors since 2013 and remains on the forefront of tackling these issues. The FBI will proudly continue to lead the U.S. Government’s efforts to combat this threat by educating employees, the public, and private and public sector partners.

[7] Passed as part of the National Defense Authorization Act of Fiscal Year 2021; and referenced in H.R. 6395, Division F-Anti-Money Laundering, Title LXIV – Establishing Beneficial Ownership Information Reporting Requirements, Sections 6401-6403.

IX. Appendix

Example Public Service Announcements

Internet Crime Complaint Center (IC3)
Public Service Announcement
May 04, 2022

Alert Number
I-050422-PSA

https://www.ic3.gov/Media/Y2022/PSA220504

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

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.

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.

Internet Crime Complaint Center (IC3)
Public Service Announcement
December 03, 2021

Alert Number
I-120321-PSA
https://www.ic3.gov/Media/Y2021/PSA211203

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Money Mules: A Financial Crisis

WHAT IS A MONEY MULE?

Any individual who transfers funds, on behalf of, or at the direction of another. Money mules are recruited to assist criminals with laundering proceeds from illegal activity and are often promised easy money for their participation in moving funds by various methods including:

- Cryptocurrency
- Physical currency (cash)
- Bank transfers (wires, ACH, EFT)
- Money services businesses
- Pre-paid cards

WAYS MONEY MULES ARE RECRUITED

- Unsolicited emails or other communications requesting to open a bank account, cryptocurrency wallet, or business in their name
- Romance/confidence scams
- Employment scams promising easy money
- Non-payment/non-delivery scams
- Lottery scams where personal information is collected

MONEY MULE: COMPLICITY

Unwitting or unknowing mules: not aware that they are involved in a bigger criminal scheme. These individuals are typically recruited via scams such as romance scams or more recently, employment scams due to the COVID-19 pandemic. Generally, these individuals genuinely believe they are helping someone who is acting as their romantic partner or employer.

Witting mules: ignore warning signs of criminal activity or are willfully blind to the financial activity they are participating in. They may have received warnings from bank personnel but continue to open multiple accounts. These individuals generally begin as an unwitting mule.

Complicit mules: aware of their role as a money mule and complicit in the larger criminal scheme. They might regularly open bank accounts at various institutions with the intention of receiving illicit funds or openly advertise their services as a money mule and actively recruit others.

WHO IS AT RISK?

Anyone can be recruited to be a money mule; however, targeted populations include the elderly, college-aged students, and newly immigrated individuals. Cyber-expertise or knowledge is not required the money mule will be directed how to open accounts and process various transactions.

RECENT TRENDS

In 2020 into 2021, the IC3 received an increase in complaints relating to COVID-19 related fraud and online scams involving cryptocurrency, such as business email compromises, extortion, employment scams and confidence/romance scams. The increases in these scams could be the result of isolation due to COVID-19 quarantine restrictions, the loss of employment due the COVID-19, and increases in remote work which allowed criminals to instruct money mules to provide copies of their personal information online.

Money mules were also asked to provide copies of their personal information or to directly open cryptocurrency accounts and wallets as part of online scams such as romance fraud, extortion, non-payment/non-delivery, or investment scams. These accounts opened in the money mule's name could then be later used in other scams to target victims of business email compromises, tech support, and other online scams.

CONSEQUENCES FOR ACTING AS A MONEY MULE

Individuals acting as money mules are putting themselves at risk for identity theft, personal liability, negative impacts on credit scores, and the inability to open bank accounts in the future. Furthermore, they and their families could be threatened by criminals with violence if they do not continue to work as a money mule.

In addition, these individuals face prison sentences, a fine or community service, even if unwitting. Particularly in the United States, potential Federal charges include: Mail Fraud, Wire Fraud, Bank Fraud, Money Laundering, Transactional Money Laundering, Prohibition of Unlicensed Money Transmitting Business, and Aggravated Identity Theft. These charges come with fines reaching $1,000,000 and up to 30 years in prison.

TIPS FOR PROTECTION

If you believe you are being used as a money mule:

- STOP communicating with the suspected criminal
- STOP transferring funds or items of value
- Maintain receipts, contact information, and communications (emails, text messages, voicemails) so the information may be passed to law enforcement

- Notify your bank or payment provider
- Notify Law Enforcement. Report suspicious activity to the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov and contact your local FBI field office

To prevent yourself from being recruited as a money mule:

- Do not accept job offers that ask you to receive company funds into your personal account or ask you to open a business bank account
- Be suspicious if a romantic partner asks you to receive or transfer funds from your account
- Do not provide your financial details to anyone (e.g., bank account information, logins, passwords)
- Do not provide copies of your identification documents to anyone (e.g., driver's license, social security number)
- Conduct online searches to corroborate any information provided to you
- Reach out to your financial institution with banking questions or concerns about financial transactions in your account

For additional information on Money Mules, please view:

FBI Scams and Safety: Don't Be a Mule: Awareness Can Prevent Crime
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules