FinCEN Director's Law Enforcement Awards Program Recognizes Significance of BSA Reporting by Financial Institutions

Category: Significant Fraud

The Financial Crimes Enforcement Network (FinCEN) holds an annual Director's Law Enforcement Awards ceremony, presenting awards to law enforcement agencies that use Bank Secrecy Act reporting provided by financial institutions in their criminal investigations. The goals of the program are to recognize law enforcement agencies that made effective use of financial institution reporting to obtain a successful prosecution, and to demonstrate to the financial industry the value of its reporting to law enforcement. The program emphasizes that prompt and accurate reporting by the financial industry is vital to the successful partnership with law enforcement to fight financial crime.

The program is open to all federal, state, local, and tribal law enforcement agencies and includes seven award categories recognizing achievements in combatting significant threats to the integrity of the financial system and the safety of our communities. One of these categories is "Significant Fraud." A brief summary of each 2020 nomination within this category is provided below.

United States Secret Service (USSS)

USSS investigators led this multi-state investigation into several purported investment firms offering high-yield energy company investment opportunities. The companies under investigation promised returns of 20-30 percent in exchange for a $50,000 investment into oil companies. Investigators relied heavily on an analysis of sensitive financial data to help establish the connections between the individuals controlling the investment firms and identify fraudulent transactions totaling over $21 million moving between 53 shell companies and 14 individuals.

USSS officials coordinated with FinCEN to produce an exhaustive list of financial institutions holding bank accounts and other leads for the investigative team to follow, including numerous transfers to various accounts in Australia. Officials leveraged the results of their coordination with FinCEN to coordinate further with the Australian financial intelligence unit. These efforts resulted in the identification of foreign bank accounts and an Australian citizen involved heavily in the fraud scheme.

A two-year forensic analysis of the financial data revealed that less than nine percent of all funds sent to the targets actually went to investment products. The three main companies that investors sent funds to utilized a large network of shell companies to launder the funds. Investigators interviewed hundreds of victims and coordinated with the Securities and Exchange Commission to assist in numerous cease and desist orders against the companies. Based on their analysis of financial data, officials determined that these same individuals had operated multiple fraud schemes in the past, defrauding investors out of over $53 million.

USSS officials executed simultaneous search warrants in Texas, Tennessee, Illinois, and Florida. Interviews with the targets of the investigation led to an admission that the companies were fronts for a fraud scheme organized by the targets and numerous other individuals with a history of fraud. USSS officials also executed 41 federal seizure warrants, eight consent searches, 32 subject interviews and seized nearly $1 million in account funds, cash, gold coins, and bitcoin.

The primary subjects of this investigation pled guilty to charges of wire fraud, mail fraud, and securities fraud.

U.S. Department of Agriculture – Office of Inspector General (USDA-OIG)

This joint investigation included numerous federal law enforcement agencies and resulted from an analysis of sensitive financial and Supplemental Nutrition Assistance Program (SNAP) data by USDA-OIG investigators.

The internal review by USDA-OIG investigators revealed that a small supermarket located in New Jersey had unusually high SNAP program sales reported for a business of that size. In addition, financial analysis revealed that there were unusually high cash withdrawals being made out of the accounts of this business, just below reporting thresholds.

Law enforcement officials determined that the subjects would allow the purchase of items, both eligible and ineligible for SNAP benefits, add an amount to the transaction that could not be accounted for by goods purchased, and provide cash back to the “customer” in exchange for SNAP benefits. A review of the tax-related documents showed that the subjects used the

SNAP totals as gross receipts even though they gave a portion of the money back to the “customers” and kept the balance of the transaction. SNAP sales were electronically deposited through Automated Clearing House transactions into a business checking account on which the subjects were authorized signers. It was determined that the rise in gross receipts also required the subjects to offset the cost of goods sold in order to reduce the tax liability for the business. The subjects conducted many large withdrawals and wire transfers in order to purchase vehicles and real estate, and shop at various retail locations for personal use. Many of the vehicles purchased were subsequently exported out of the country to the Dominican Republic.

Investigators determined that over a four year period, the primary subjects defrauded the SNAP program, engaged in significant money laundering and committed tax fraud. The subjects pled guilty to all charges and agreed to pay full restitution of over $4.8 million to the U.S. Department of Agriculture’s Food and Nutrition Service and over $400,000 to the Internal Revenue Service.

U.S. Customs and Border Protection (CBP)

This multi-agency investigation began when the Department of Homeland Security – Office of Inspector General (DHS-OIG) received a complaint alleging that an Immigration and Customs Enforcement – Homeland Security Investigations (ICE-HSI) Special Agent, with the assistance of his wife, conspired in a scheme to engage in bank and mortgage fraud. The subjects laundered and structured deposits of U.S. currency and evaded payment of federal and state taxes in connection with a property management business they co-owned.

DHS-OIG investigators received a secondary allegation that the primary subject, under the guise of a law enforcement seizure, stole an undetermined amount of illicit funds derived from drug trafficking from two individuals employed by drug traffickers during a vehicle stop in California. Investigators utilized a wide range of techniques to collect, identify, and analyze leads. An analysis of sensitive financial information revealed that the subject used criminally obtained funds to make real estate purchases, travel internationally, gamble at casinos, and furnish homes. A review of tax records showed the subjects had not filed state or federal tax returns in many years.

Investigators accumulated enough evidence to execute four simultaneous search warrants on the subjects' personal residence, assigned government vehicle, and government and personal cell phones. Among the items seized were 15 boxes of documents relating to over 30 real estate properties owned by the subjects, banking documents, U.S. currency in the approximate amount of $13,000 and other documentary evidence. Immediately preceding the execution of the search warrants, the primary subject was interviewed by investigators and made numerous false statements. Following the questioning and the search of his residence and government vehicle, he took a six month leave of absence and subsequently resigned from his position.

Additional financial analysis determined that the subjects continued to make large cash deposits into bank accounts and open additional accounts in foreign jurisdictions. Investigators subsequently executed an additional search warrant based on evidence related to tax evasion, money laundering, fraud, and firearms violations. Simultaneously, pursuant to a criminal complaint, the subjects were arrested at a Los Angeles airport, as they were returning from vacationing in Australia. After two search warrants, several interviews, and years of financial analysis, it was determined that the subjects' business was not generating the amount of income deposited into their bank accounts.

The investigation resulted in a 38-count indictment, including counts of money laundering, structuring, lying to federal agents, conspiracy to commit bank fraud and tax evasion. The primary subject's wife pleaded guilty to conspiracy to commit mortgage fraud and provided limited cooperation against her husband. After two years of post-indictment litigation, the primary subject pleaded guilty to 19 counts, including money laundering counts and false statements to federal agents.

U.S. Department of Justice – Consumer Protection Branch

This money mule initiative began when Federal Bureau of Investigation (FBI) officials initiated discussions with the goal of identifying money mules who were facilitating large-scale criminal fraud schemes, especially those involving transnational elder fraud. FBI, the U.S. Postal Inspection Service, and U.S. Department of Justice's Consumer Protection Branch led the initiative and successfully encouraged other federal and state counterparts to join the effort.

Given obstacles to the use of traditional law enforcement tools to identify and prosecute transnational fraud schemes, agents and prosecutors have sought unconventional and creative ways to stem the tide of victim losses resulting from those schemes. Much these efforts focuses on money mules—critical contributors to the schemes who work and reside within the United States. Law enforcement recently has employed various strategies, ranging from warnings to prosecutions, to deter mule conduct, depending on each individual mule's culpability.

Law enforcement officials from numerous agencies analyzed extensive sensitive financial records as part of this initiative and identified an extensive list of money mules. They deconflicted each money mule to protect against harming ongoing criminal investigations within their own agencies and others. Once money mule leads were cleared, the nominees referred leads to field agents, who took action. The vast majority of actions consisted of knock-and-talk interviews and service of warning letters, informing the money mules that they were facilitating criminal schemes. Agents warned the mules that continued mule activity could result in criminal prosecution. Recent analysis has indicated that approximately 80 percent of money mules who receive warning letters stop facilitating fraud. It is impossible to quantify the fraud losses disrupted by this money mule initiative.

The actions taken by law enforcement officials halted the conduct of more than 600 money mules, spanning over 85 federal districts. Actions addressed a variety of elder fraud scheme types, including romance scams, lottery and sweepstakes scams, Internal Revenue Service and Social Security Administration imposter scams, veteran and Social Security benefit redirection scams, and technical support scams. Law enforcement officials interviewed more than 550 individuals and served over 500 warning letters to individuals who recently served as money mules for fraud schemes. The letters informed recipients that they could be prosecuted if they continue aiding and abetting fraud schemes. More than 30 individuals were criminally charged for their roles in receiving victim payments and providing the fraud proceeds to accomplices.

Federal Bureau of Investigation (FBI)

This investigation was initiated and predicated on multiple complaints from investors who were not receiving their promised interest payments from what they believed to be a legitimate investment firm. The subjects of this investigation were the managing directors of a company based in Florida that solicited and raised approximately $150 million from investors worldwide, including more than $64 million from investors in the United States. Investors were promised a rate of return of 12-24 percent. In reality, investor funds were used to pay other investor returns, broker commissions, and funded other companies owned by the subjects, including a catering

company, a travel agency and a food truck business. The owners of the company opened offices and affiliates around the world, including in London, Hong Kong, Taipei, Shanghai, Singapore, Vancouver, and Panama.

Many of the investors were elderly individuals utilizing retirement savings for the investments. The investigative team interviewed dozens of investors during the course of this investigation who suffered substantial financial hardship due to their "investments" with the subjects. Actual losses to U.S. investors are approximately $49.7 million. The Securities and Exchange Commission filed a complaint against the company, and it subsequently filed for bankruptcy, claiming estimated assets totaling less than $50,000.

The analysis of sensitive financial information and the cooperation of financial institutions greatly assisted the investigative team in dismantling the investment fraud scheme.

Investigators discovered that financial institutions had notified the subjects of their anti-money laundering policies and procedures. These notifications played a significant role in determining that the subjects were engaging in money laundering while on notice from the banking industry, yet they continued to engage in the same activity at numerous financial institutions.

FBI Special Agents coordinated investigative efforts with multiple foreign law enforcement agencies, resulting in the discovery of valuable intelligence and the arrest of multiple individuals in foreign jurisdictions. U.S. authorities arrested the three primary subjects of this investigation, and they were sentenced to 12 to 240 months in federal prison and ordered to pay over $150 million in restitution.

U.S. Postal Inspection Service (USPIS)

An investigation led by the USPIS uncovered an international organized fraud ring operating primarily from Jamaica, with numerous co-conspirators strategically placed throughout the United States, including a concentration of criminal associates located in the Florida panhandle. The fraud ring targeted elderly victims and induced them to send money with false promises of sweepstakes prizes. The organization's modus operandi involved receiving victim proceeds that were wired via money transfer services or express mailed via the U.S. Postal Service or other interstate carrier. The criminal proceeds were then cashed and wired to co-conspirators in Jamaica or bulk cash smuggled during periodic trips back and forth to Jamaica.

Investigators relied heavily on financial data analysis and inspections to establish justification for a search warrant. The search warrant resulted in the seizure of thousands of dollars in cash, along with computers and cell phones the subjects used to carry out their fraud scheme. Subject interviews revealed that they received packages containing money from victims, which they would keep a portion of, then wire the rest of the funds to Jamaica. The subjects stated that the main organizers of the scheme in Jamaica provided directions on where to wire the money.

A grand jury returned a 17-count indictment charging the subjects in mail fraud, wire fraud, and conspiracy for this scheme involving amounts in excess of $400,000. Two of the subjects were sentenced to prison terms of 36 months, followed by 36 months of supervised release. The third

subject was sentenced to a term of 30 months of imprisonment and 30 months of supervised release upon completing his prison sentence.

An in-depth analysis of sensitive financial data provided law enforcement with a helpful lead on which businesses to subpoena records from; and together provided law enforcement with an accurate understanding of the fraud scheme, the criminal targets, and their organizational structure. The data helped to identify the methods the fraud ring used to launder money from victims to criminal co-conspirators in the United States and ultimately to the ringleaders in Jamaica.

Drug Enforcement Administration (DEA)

DEA officials led this multi-agency investigation comprised of numerous federal, state, and local law enforcement agencies. The investigation began when several DEA offices contacted the Baltimore, Maryland office for assistance identifying an illegal controlled substance source of supply in the Baltimore area. The source of supply was providing counterfeit pharmaceutical pills to targets of several individual investigations.

Research and financial data analysis identified the target and revealed that he and several co-conspirators' suspicious financial activity had recently captured the attention of several banks and money services businesses. During the course of the investigation, DEA and USPIS officials were able to identify several postal meters that were utilized to assign postage on packages of controlled substances sent throughout the United States. The information from USPIS allowed case agents to track the packages that entered the mail system. Surveillance efforts led to the discovery of large bags containing counterfeit pharmaceuticals and fentanyl, as well as ingredients used to manufacture pharmaceuticals.

The Drug Trafficking Organization (DTO) used customers on the "dark web" marketplaces to sell counterfeit pharmaceuticals and received payment via bitcoin. Extensive surveillance and investigative efforts led to the discovery that the primary subject was utilizing his parents' residence to manufacture counterfeit pharmaceuticals and ship it out to dark web customers. Based on additional financial forensic analysis, investigators identified 40+ dark web-based virtual currency accounts, owned and operated by the DTO to facilitate its money laundering network. In addition, the primary subject was utilizing an addiction recovery center in Maryland to help launder his drug proceeds.

The investigation culminated when multiple law enforcement agencies executed five federal search and seizure warrants and two arrest warrants. Two primary subjects were arrested at their respective residences, which were subsequently searched. Law enforcement officials seized bitcoin and other cryptocurrency valued in excess of $16,180,000, approximately $2,000,000 in U.S. currency, computer hardware worth in excess of $1,000,000, one pill press, large amounts of counterfeit pharmaceuticals, and small amounts of other drugs to include fentanyl, 11 weapons, and two vehicles.

The subjects were indicted on numerous drug manufacturing, possession, and distribution charges. The primary subject was sentenced to a 57-month prison term and three years of supervised release. A second subject was sentenced to 11 months of supervised release, including eight months of home confinement.