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

Category: Third Party Money Launderers

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 "Third Party Money Launderers." A brief summary of each 2020 nomination within this category is provided below.

U.S. Immigration and Customs Enforcement – Homeland Security Investigations (ICE-HSI)

This multi-agency investigation led by HSI and Internal Revenue Service, Criminal Investigation (IRS-CI) agents targeted a foreign national who is the daughter of a high ranking foreign political official and three multi-national companies for Foreign Corrupt Practices Act money laundering violations. An extensive analysis of financial data identified a multifaceted organization that had numerous entities all sending money to select companies with multiple bank accounts around the world.

Investigators coordinated with numerous financial intelligence units to help identify and prioritize individuals and companies and their foreign financial institutions where law enforcement could turn for investigative assistance. The investigation identified several

foreign telecom companies, all of which were traded on U.S. stock markets, offering bribes and kickbacks to the individual subject in exchange for telecom contracts. The funds related to corrupt acts were subsequently laundered through the U.S. financial system.

The investigation proved that the subject telecom companies entered the market by making large payments to shell companies owned by the individual subject. The companies continued to pay bribes to the subject through complex international transactions in order to remain in the subject's favor and continue operations. As a result of investigative efforts, the United States successfully froze approximately $850 million in accounts held overseas that were directly traced to bribe proceeds paid from the telecom companies to the individual subject, which were subsequently seized as money laundering proceeds.

Over the course of the investigation, the United States and international partners settled with each of the telecom companies for civil penalties totaling $2.7 billion, to include $120 million in criminal forfeiture. Foreign authorities also indicted three key executives of the telecom companies, while the primary subject of the investigation and her chief lieutenant were both indicted by the United States on money laundering charges.

Federal Bureau of Investigation (FBI)

This business email compromise (BEC) investigation began after the victim company contacted the FBI to request assistance investigating the fraud and inquiring about a wire recall.

The fraud scheme started when an administrative assistant at the victim company received an email containing an invoice that was purportedly from the representative of a company known in an official business capacity to the victim company. The invoice amount referenced in the fraudulent email was over $80,000. The victim sent an $80,000 wire transfer to the subject's account in London, but the subject subsequently asked the victim to recall the wire transfer and instead send the $80,000 to a different account. FBI investigators determined that the subject requested the recall because the original account had been frozen by the receiving financial institution due to suspicious activity.

During the extended period of time it took for the victim to receive their funds back, the management team of the victim company discovered the fraud scheme and requested FBI assistance. During victim interviews and an analysis of supporting documentation, including the email communications and wire instructions, FBI investigators determined that the subject was using their account to carry out numerous separate frauds at the same time and thus the account had been frozen by the financial institution.

FBI officials coordinated with the UK financial intelligence unit to obtain additional information about the subject. As a result of their efforts, FBI officials successfully assisted in recalling all but $3,000 of the victim's original wire transfer and identified the subjects operating in London and elsewhere.

Federal Bureau of Investigation (FBI)

FBI and United States Attorney's Office officials initiated an investigation predicated on a business email compromise (BEC) scheme in which the subject duped a construction company based in Texas to send more than $210,000 to a fraudulent account in the state of Washington.

FBI investigators identified the subject and several co-conspirators, along with significant wire transfer activity through an analysis of financial data and coordination with the South African financial intelligence unit. FBI forensic accountants conducted extensive financial analysis throughout the investigation, which concluded that the subject and other known and unknown co-conspirators were third-party money launderers who layered financial transactions and created false documentation to open shell companies in support of their fraudulent activity. The investigation uncovered false tax returns, fraudulent mortgage loans and merchant account fraud. The primary subject opened at least five fraudulent businesses to process stolen credit card account numbers via multiple merchant services providers at various banks.

Based on the financial analysis, FBI officials determined the subject had facilitated financial fraud for more than six years, and schemes ranged from credit card merchant fraud to check kiting to BEC. The total loss amount in the investigation was over $1 million; however, the total intended loss was several million dollars. Law enforcement officials served over 40 subpoenas throughout the investigation and obtained financial records that helped identify additional schemes, transactions, and bank accounts.

Law enforcement officials obtained search warrants for multiple email accounts in order to identify additional subjects, victims, and impacted financial institutions as well as other evidence material to the investigation. Investigators subsequently obtained a criminal complaint against the primary subject for money laundering offenses, and traveled from Texas to the state of Washington to coordinate arrest and search warrants. During his initial appearance in the Western District of Washington, the subject waived his detention and identity hearings and was transported to the Southern District of Texas, where the Judge ordered him detained pending trial. The subject eventually participated in a proffer agreement, which outlined various large-scale fraudulent activities occurring over the last 10 years, to include not only numerous BEC schemes, but also frauds related to cryptocurrency, prepaid cards, and $900,000.00 in fraudulent checks. In late 2019, the subject's defense attorney requested a plea agreement to conspiring to commit money laundering. The statutory maximum penalty is imprisonment of not more than 20 years.