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

Category: SAR Review Task Force

The Financial Crimes Enforcement Network (FinCEN) holds an annual 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 "SAR Review Task Force." A brief summary of each 2018 nomination within this category is provided below.

Internal Revenue Service-Criminal Investigation Division (IRS-CI)

This case, led by IRS-CI investigators, began when a task force officer from the South Florida Financial Crimes Strike Force identified a financial data revealing a high volume of possible illegal activity. This data helped develop the case into a large-scale international mail fraud and money laundering investigation led by IRS-CI and U.S. Postal Inspection Service Special Agents.

The subjects of the investigation were carrying out a lottery fraud scheme, sending mailings to individuals in 20 countries stating that the recipient had won a prize of several million dollars. In order to receive the prize, the recipients had to pay a $20-$40 processing fee. The majority of recipients were elderly individuals. The scheme generated $28 million in illicit proceeds from hundreds of thousands of victims around the globe.

The subjects maintained hundreds of bank accounts, at least 50 P.O. boxes, and at least 70 shell companies to conceal the true identity of the individuals and location of the funds. The bank accounts were held in the names of the various shell companies and opened by low level operators, while being completely controlled by the organizers.

Several domestic bank accounts were used to receive victim payments. Investigators were able to use data from these transactions and accounts to piece together financial trails and identify victims. Investigators used information discovered amongst a high volume of transactional data to identify over $2.5 million that was laundered through U.S. bank accounts.

Law enforcement agencies from several countries assisted in the investigation, arresting several individuals and testifying during trial. The members of the criminal group were indicted on mail fraud and money laundering charges, among others. One of the subjects plead guilty, while all of the remaining subjects went to trial and were convicted.

Homeland Security Investigations (HSI)

This case was initiated when HSI agents began investigating funnel account activity that was identified in a review of sensitive financial information. This data indicated that a personal bank account was being utilized to funnel illicit funds across the United States. The data helped launch a lengthy investigation into Mexico-based professional money launderers who were laundering millions of dollars in drug proceeds from the United States to Mexico.

The initial financial data enabled investigators to obtain additional documentation from several financial institutions being used by the targets of the investigation. Physical surveillance and monitoring was conducted on the individuals accessing bank accounts at several branch locations and officials were able to develop additional resources to help further their investigation. Surveillance revealed that the targets frequently visited a number of money remitters, both licensed and unlicensed, to help launder the drug proceeds to Mexico. Agents learned that the money remitters were complicit in the scheme and agreed to structure transactions to avoid reporting requirements and falsify sender and receiver information.

The transaction records discovered by investigators played a crucial role in the investigation and prosecution of the targets of this investigation. HSI officials apprehended and were able to obtain guilty pleas from nine individuals to various money laundering and conspiracy charges. Two other individuals have been charged with money laundering and conspiracy, but have not yet been apprehended.

Internal Revenue Service-Criminal Investigation Division (IRS-CI)

IRS-CI officials kicked off their investigation when multiple financial institutions became suspicious of the activity generated through the merchant dealer accounts the subject had established to offer lines of credit to customers of his furniture stores. Over a four-month period,

the subject submitted over 250 credit card applications charging over $3.3 million to two banks that were allegedly completed by customers.

Investigators learned that the subject of this investigation fraudulently completed all of the credit card applications, using the personal identifying information of recently deceased individuals. A review of transaction records revealed that the subject transferred the funds received as credit lines to his business account at another financial institution. From there, he withdrew the funds and immediately deposited them at various casinos located in Arizona and Nevada. Once the funds were deposited at casinos, he cashed out the funds with minimal to no gaming activity. The subject also used money orders to make occasional payments towards the credit lines in the names of deceased individuals.

Investigators from IRS-CI, the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement-Homeland Security Investigations, and the U.S. Attorney's Office determined that the subject had previously been involved in a large-scale loan fraud scheme. Prior to the furniture business ventures, the subject was a purported real estate investor who operated a company that would purchase foreclosed properties, rehabilitate them, and sell them for profit. The subject falsified documents, including purchase agreements for several thousand loans from a single lender. The funds were made payable to the subject himself, and ultimately used for personal gain. The lender was defrauded out of approximately $47 million as a result of the loan fraud.

The subject of this investigation, along with one co-conspirator, was indicted on bank fraud, wire fraud, identify theft, and money laundering charges. The subjects pled guilty to the charges and the primary subject is currently servicing a 17-year prison sentence and was ordered to pay over $33.5 million in restitution.

Defense Criminal Investigative Service (DCIS)

DCIS officials initiated this investigation based on an analysis of financial data identifying the subject, who was a Staff Sergeant in the U.S. Army Reserves (USAR), as the individual behind a bribery and corruption scheme involving over $1 million in government contracts.

Initial information acquired by DCIS officials revealed a pattern of unexplained ATM deposits totaling nearly $84,000 to an account belonging to the subject. Investigators determined the subject was cashing money orders through another personal account and depositing the cash through ATMs. Investigators traced the origin of the money orders to a company located in California. They further determined that their target ordered $1.2 million worth of supplies from a third company, which subsequently funneled cash and checks to the company that had been purchasing the money orders as kickbacks for the subject in response to supply orders. Investigators later determined that the owner of the supply company also provided supply purchases, including the subject of this investigation, with gift cards, rebate, and other gratuities for purchases made through his company.

The supply company owner was charged with bribery of a public official for providing more than $80,000 to the subject in exchange for $800,000 worth of equipment for the U.S. Army. He was sentenced to five months in prison and a forfeiture of $95,000. The primary subject was charged with accepting and receiving a gratuity and sentenced to eight months' incarceration and a forfeiture of $95,000.

United States Secret Service (USSS)

USSS investigators began their investigation on a tip regarding a possible large-scale Ponzi scheme. Based on the information received in the tip, investigators analyzed financial documents and discovered multiple indicators of money laundering activity. The data indicated that the subject was operating a penny-auction site, where bidders are charged a small non-refundable fee for each bid they place on an item. The company makes money from the fees charged for each bid as well as the profit from selling the items for more than they were originally acquired.

Investigators scoured large volumes of account and transaction data, and relied on cooperation and analysis from FinCEN and other foreign financial intelligence units (FIUs) to help piece together the financial trail in this case. As a result of these efforts, investigators identified funds movement through 15 different bank accounts located in the United States, Canada, Australia, and Moldova. An analysis of supporting documentation received from these financial institutions showed that the company had a very small volume of sales and auctions, but had large cash deposits coming in from various individuals. It was determined that these large cash deposits were coming from scam victims induced to invest in a Ponzi scheme, where the victims were convinced that the company was generating millions of dollars in legitimate profits from its auction site and the investors would be included in a "profit pool," earning returns of 125% on their investments.

USSS investigators coordinated with IRS and U.S. Securities and Exchange Commission officials to determine the subject defrauded victims of $985 million and utilized those funds for personal expenses and to pay previous investors. The financial records proved critical in recovering nearly $300 million for victims. The subjects of this case were indicted on various fraud and conspiracy charges. Several subjects pleaded guilty to the charges while another subject went to trial and was found guilty on all counts.

United States Secret Service (USSS)

This proactive case originated upon a referral from the USSS's Criminal Investigative Division by utilizing sensitive financial information to identify a money laundering scheme. The results of the investigation led to multiple arrests and significant asset forfeitures.

The subjects of this investigation operated shell companies that were used to facilitate a scheme in which they purported to purchase renewable fuel from co-conspirators in order to obtain credits from the U.S. government. The subjects then used a series of false transactions to convert

the proceeds of the fuel back into materials needed for the production of renewable fuel and sold them back to their co-conspirators, allowing the credits to be claimed again. The proceeds of the criminal activity were then laundered through bank accounts in the names of multiple shell companies.

Over a 12-month period, the subjects fraudulently generated enough credits to receive over $42 million from their sale. In addition, the co-conspirators received over $4.3 million in false tax credits as a result of the scheme.

USSS officials, in coordination with several other Federal law enforcement agencies, analyzed financial data to identify suspicious transactions involving the subjects and several co-conspirators. This data detailed $97 million in suspicious activity during a one-month period, comprised of wire transfers and checks between what appeared to be shell companies.

Agents issued simultaneous search and seizure warrants at multiple facilities and residences in the multiple states. These warrants resulted in the seizure of over $7.2 million in cash, gold coins, monetary instruments, bank accounts, jewelry, vehicles, and real property. Based on the information identified in the financial data, as well as the results of the warrants, the subjects were arrested on money laundering and wire fraud charges and subsequently sentenced to 10 to 11 years in prison.

United States Secret Service (USSS)

USSS officials analyzed a significant amount of financial data to identify suspects, businesses, and the movement of money by a criminal organization participating in a health care fraud and money laundering scheme.

Investigators were also able to identify financial institutions with information that helped further their investigation during their data analysis. Supporting documentation obtained from the financial institutions identified several companies that purported to provide home health services to Medicare beneficiaries. The subjects of this investigation attempted to conceal the true ownership of the companies by using nominees and a series of shell companies. Over a 3-year period, the companies received nearly $10 million in Medicare reimbursements.

USSS agents coordinated with agents from several other law enforcement agencies to conduct search warrants on one of the companies, where extensive documentation and evidence was discovered and interviews were conducted. The results of these search warrants and the account and transaction records identified a network of 12 companies used to facilitate the fraud scheme.

The subjects of this investigation arrested and plead guilty to various fraud and money laundering charges. Several of the subjects were apprehended while trying to enter the United States with $2.4 million hidden in their luggage and subsequently plead guilty to smuggling charges as well. The two primary subjects of the investigation were sentenced to 135 and 151 months in prison, respectively for their roles in the $20 million fraud conspiracy that involved

paying illegal kickbacks to patient recruiters and medical professionals. The subjects were ordered to pay $22.9 million in restitution and seizures totaled an additional $3.7 million.

U.S. Attorney's Office-Oklahoma

Agents from several Federal law enforcement agencies initiated this investigation after identifying multiple sources of sensitive financial information concerning the money laundering activities of their subject. The financial information initially revealed over $1 million in large cash transactions through the subject's accounts, as well as large check deposits from a smoke shop and outgoing wire transfers to a pharmaceutical company in China. Investigators used the data and subsequent supporting documentation to determine the subject was selling synthetic cannabinoid products through online marketplaces, describing it as "aromatic potpourri."

Investigators received information from various sources, including state and local law enforcement agencies, indicating that their subject was responsible for the manufacturing and distribution of synthetic cannabinoids in Oklahoma. A further analysis of financial data was conducted using new information received from state and local agencies, and investigators were able to identify additional financial accounts and transactions involving their subject. The newly discovered transactions included payments to and from various manufacturing and raw material supply companies in the United States, and China. Investigators concluded that the sales of synthetic cannabinoid totaled over $8 million over an 18-month period.

Search and seizure warrants were executed on the subject's properties, which corroborated the $8 million sales figure. Agents also discovered over $1.8 million in cash and a large amount of silver bars during the execution of the search warrants. The subject's residence was seized during this process and he subsequently plead guilty to money laundering and conspiracy charges. The subject faces 5 years in prison and a $250,000 fine, along with a $1.7 forfeiture agreement.

High Intensity Drug Trafficking Area Task Force – Northern Virginia Financial Initiative

Officials from various Federal, state, and local law enforcement agencies initiated an investigation into possible money laundering and contraband cigarette smuggling by the owners of a small gas station.

Investigators determined that shortly after purchasing the gas station, the subjects began trafficking contraband cigarettes from Virginia to New York using the gas station to purchase them at wholesale prices. The subjects registered a shell company in New York that was used to launder the proceeds of the illicit activities. Over a 2-year period, the subjects purchased over $7 million in cigarettes to be re-sold in New York.

Investigators poured over a high volume of financial documents to identify a clear pattern of cash structuring and various schemes to avoid reporting and tax compliance requirements. This

information helped investigators obtain search warrants on the subjects' business, recovering over $172,000 in cash, along with other evidence. The primary subject pled guilty to trafficking in contraband cigarettes, and consented to a $1 million forfeiture and other tax and fine penalties. He was sentenced to 2 years in Federal prison. Several other subjects also pled guilty to their roles in the criminal activity and were subjected to nearly $6 million in penalties and fines.

Drug Enforcement Administration (DEA)

DEA investigators discovered a narcotics distribution operation while analyzing sensitive financial data for potential criminal activity. The operation was led by an individual identified as having conducted over $780,000 in transactions during a 2-year period, many of which were cash deposits. The transaction records outlined a pattern of out-of-state cash deposits immediately followed by cash withdrawals. The documentation identified four different bank accounts controlled by multiple subjects.

After an arrest by local law enforcement for operating an indoor grow operation, the primary subject continued the out-of-state cash deposits, but the funds were more frequently being transferred to a chemical company in Hong Kong. DEA officials identified packages sent from the Hong Kong company to associates of the primary subject located in the United States. The packages were all mislabeled to disguise the narcotics contained inside. Investigators identified 50 shipments from Hong Kong during their investigation, which allowed them to obtain a search and arrest warrant on the subject. Seizures included narcotics processing materials, cocaine, over $200,000 in cash, and several high-end vehicles, boats, and pieces of jewelry. The subject and several co-conspirators were arrested on money laundering, drug trafficking, and drug manufacturing charges.

U.S. Customs and Border Protection (CBP)

Through coordination with several Federal law enforcement agencies, CBP agents became aware of six individuals, with previously unknown identities, opening bank accounts with different aliases and fraudulent identification documents throughout Rhode Island. The purpose of the fraudulently opened bank accounts was to launder the proceeds of their fraud scheme against U.S. citizens.

CBP officials were able to identify the subjects through an analysis of financial data and shipping records. The data helped identify 49 fraudulently opened bank accounts, along with countless addresses and phone numbers for the subjects. The subjects of this investigation defrauded 10 banks out of over $850,000 by acquiring and altering checks that had already been passed between commercial entities. The checks were altered to be made out to aliases and deposited into the accounts that were fraudulently opened. In most instances, the funds were subsequently removed from the accounts prior to the fraud being detected by the financial institutions. The subjects also sent unauthorized wire transfers into these accounts, which were followed by rapid withdrawals.

Collaboration with FinCEN and several law enforcement agencies enabled CBP officials to identify and arrest the subjects for their participation in this large-scale counterfeit bank account and identification scheme. The subjects have been charged with bank fraud, passport fraud, identify theft, and access device fraud.