FinCEN Awards Recognize Law Enforcement Success Stories Supported by Bank Secrecy Act Reporting

Category: Significant Fraud

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 six 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 2017 nomination within this category is provided below.

Immigration and Customs Enforcement (ICE-HSI)

HSI officials initiated an investigation into a business and its operators after investigators discovered a high volume of sensitive financial information indicating this organization appeared to be laundering millions of dollars through accounts at multiple financial institutions. The financial data revealed several individuals and shell companies using a single, third-party company to launder illicit funds. Based on information indicating large-scale money laundering through this third-party company, investigators issued a series of warrants, resulting in the seizure of over $625,000.00 from a single account, multiple vehicles, and a large amount of documentation evidencing the money laundering activities. The suspects targeted in this phase of the investigation were charged with various money laundering offenses and all pled guilty.

The evidentiary documentation obtained through seizure led to the identification of additional subjects, who were also indicted and convicted of various money laundering charges and subject to $160,000 in seizures.

As a result of analyzing information obtained during the first phase of this investigation, officials discovered an organization consisting primarily of illegal aliens conspiring with the target company to launder fraudulently obtained income tax checks through this business. An analysis of sensitive financial information, as well as information obtain from confidential informants (CIs) revealed that a group of individuals was facilitating a fraud scheme through a series of businesses, ultimately laundering the funds through the investigator's primary target business. Various surveillance and analysis provided evidence of a multimillion dollar money laundering conspiracy. As a result, investigators executed 13 warrants, arresting over a dozen individuals on various fraud, identify theft, and money laundering charges. Over $400,000.00 in currency and vehicles were seized during this phase of the investigation. All individuals pled guilty.

Investigators were able to obtain cooperation from many of the individuals previously arrested to obtain information on their primary business target and the money laundering activities associated with it. This information, along with data obtained through further analysis of sensitive financial information again indicated millions of dollars in illegal proceeds. Investigators obtained search warrants for the business, the residence of the owners, and several safe deposit boxes associated with the business. Twenty seizure warrants were also issued, leading to the seizure of $5.2 million. The businesses and individuals controlling them were indicted on multiple money laundering and tax violations. The individuals operating the business both pled guilty to all charges.

Naval Criminal Investigative Service (NCIS)

NCIS officials received sensitive financial information indicating a retired U.S. Marine Corp Chief Warrant Officer was receiving unusual cash deposits to his personal accounts from various banks located throughout the United States. A joint investigation with DCIS officials was initiated and it was discovered that the locations of the cash deposits often corresponded with the subject's official travel locations. Over an 18-month period, these cash deposits totaled over $350,000.

As part of the subject's official duties, he was tasked with traveling to various military locations to inspect facilities and operations. Investigators determined that the subject was submitting travel re-imbursement claims for personal travel. Several U.S. and foreign law enforcement authorities conducted various types of surveillance to confirm that many of the travel claims were fraudulently submitted because he was not conducting any official business on these trips. Investigators were able to prove that the subject forged his supervisor's signature, and created false documents to obtain travel approval. They also confirmed that the subject was the one making the cash deposits at banks located throughout the country.

The subject ultimately pleaded guilty to wire fraud and was sentenced to a year in prison, 3 years of supervised release, and ordered to pay nearly $200,000 in restitution.

Office of the Special Inspector General for Afghanistan Reconstruction (SIGAR)

SIGAR officials opened an investigation into their subject after discovering a series of large wire transfers from an entity located in Jordan to his account at a small credit union in Oklahoma. The subject was a retired U.S. Army major who was employed as a civilian contracting officer deployed to the Middle East for several years to solicit, award and manage U.S. Government contracts.

The information discovered in an analysis of sensitive financial information led officials to conduct a more thorough investigation of the subject's personal behavior and contacts. These efforts revealed the subject, while on official duty, was approached by a foreign national who offered $1 million for help in securing U.S. Government contracts for companies the foreign national owned. The subject subsequently helped secure 12 U.S. Government contracts, valued at over $28 million for this individual and received nearly $500,000 in wire transfers during a 3 year period as payment.

Investigative officials served 15 Grand Jury Subpoenas and 2 Inspector General Subpoenas as part of this investigation, in addition to a search warrant. As a result of the investigative efforts of DCIS investigators, the subject waived indictment and pleaded guilty to bribery and tax fraud charges, resulting in the termination of his employment and security clearance, as well as a 30-month prison sentence and nearly $700,000 in forfeitures and restitution.

U.S. Department of Housing and Urban Development – OIG

HUD-OIG officials began their investigation into the Executive Director of a HUD-administrated sub-agency after HUD-OIG officials became aware of information regarding irregularities at the sub-agency. The irregularities were brought to the OIG's attention by a building contractor who claimed that the Executive Director of the sub-agency asked the contractor to include renovations to the personal residence of the Executive Director and her husband in the contract written to perform renovations on other agency-constructed residential units. Investigators interviewed additional contractors, who indicated they received agency funds from the subjects, cashed the checks, and returned a portion of the cash back to the subjects. In many instanced, no work was actually performed by the contractors. Investigators further determined that the subjects used agency credit cards and checks for personal gain, in addition to the various fraud schemes.

Based on the results of an analysis of sensitive financial information and accounting records, investigators issued search warrants at both the agency offices and the personal residence of the targets. During the search of the home, investigators discovered nearly $150,000 in cash, 44 firearms, marijuana, and other narcotics. Subsequent seizures included over $400,000, vehicles, and boats.

As a result of the investigation the subjects pleaded guilty to fraud and money laundering charges. All assets related to these charges have been seized or forfeited and sentencing is pending as of September 2017.

U.S. Postal Inspection Service (USPIS)

A review of sensitive financial information led USPIS officials to open an investigation into an individual who appeared to be carrying out some form of an elder financial abuse fraud scheme. Investigators identified check deposits into the accounts of the subject that appeared to be investments made by elderly individuals. These checks were all payable to one of three companies operated by the subject and referenced investments in the check memo lines. Investigators determined however, that these funds were being withdrawn for personal use. Debits from these accounts included cash withdrawals, vehicle purchases, and various debit card purchases.

Investigators determined that the subject encouraged victims to invest their money with her for annuities to reduce their assets below the threshold to qualify for benefits from Medicaid and the Department of Veterans Affairs (VA). The subject promised victims high returns once their incomes were reduced enough to qualify for the benefits. The subject accepted the funds from victims without ever investing the funds or filing any paperwork with the VA.

Investigators identified over $2 million the subject defrauded from investors and used for personal expenses. The subject was indicted on nineteen counts, including mail fraud, wire fraud, and money laundering. The subject subsequently pleaded guilty and was sentenced to 78 months in prison and ordered to pay restitution of over $2 million to her victims.

Internal Revenue Service-Criminal Investigation (IRS-CI)

The subjects of this investigation owned and operated an automobile salvage and recycling business, where they would purchase inoperable vehicles, strip them, and sell the usable parts and components to businesses in the secondary auto parts market. They would then sell the remainder as scrap metal.

IRS-CI officials became aware of the financial activities of these individuals and an analysis of sensitive financial information indicated that the subjects used check cashing companies to cash checks received from clients and subsequently made many large cash deposits and withdrawals. This enabled the subjects to keep transactions “off the books” and vastly underreport their sales on tax returns.

Investigators determined that the company generated over $28 million in sales over a 4-year period while only reporting $4 million on their Federal tax returns during this same period. Investigators identified 10 properties valued at $2.5 million and additional property, including vehicles, jewelry, and other personal expenditures of over $3 million during this period.

The two subjects of this case were sentenced to prison terms of 78 months and 48 months, respectively, and ordered to pay $1.5 million in restitution.

Department of Veterans Affairs - OIG (VA-OIG)

An interagency investigative team, consisting of officials from several Federal agencies, including the VA-OIG, initiated an investigation into its subjects after a contracting company

made a complaint alleging that the subjects committed fraud on surety bonds related to a Federal contract. Surety bonds are required for certain government construction contracts to ensure completion of the work in the event the contractor defaults. These bonds are obtained by the contractors on any contract exceeding $100,000 and the government reimburses the bonding fees to the contractors.

Over a 5-year period, the subject of this investigation provided fraudulent, surety bonds for Federal, state, local and private entity construction contracts. These bonds were falsified and backed by non-existent assets, including billions of dollars of purported property that actually belonged to unrelated parties. In return for these bonds, the subjects received fees from the government totaling over $6 million.

An analysis of sensitive financial information helped officials confirm the identities of the subjects and their companies as well as identify associates, assets, and accounts at various financial institutions.

The subjects of this investigation used the proceeds of their fraud scheme to purchase million-dollar homes, luxury vehicles, and jewelry, among other things.

The subjects were indicted on various fraud and conspiracy charges, sentenced to varying prison terms and ordered to pay a total of nearly $10 million in restitution and forfeitures.

Florida State Attorney's Office (SAO)

This investigation was initiated by Miami-Dade State Attorney's Office investigators and involved multiple state and local law enforcement agencies. The case was opened upon the discovery of sensitive financial information indicating the subject of the investigation conducted a series of irregular cash transactions through his account at a credit union.

The financial data helped investigators determine that the subject and his co-conspirators carried out a 5-year scheme wherein they corrupted the competitive bid process for contract work in the state. This kickback scheme led government agencies to vastly overpay for equipment that was priced at more than double their actual wholesale value. This provided the subject and his co-conspirators with millions of fraudulently obtained profits and unreported income. The government employee in charge of collecting and tallying bids to determine the lowest bidder received thousands of dollars in kickbacks in this scheme. On several occasions, the equipment orders were not filled or they were filled with equipment that the government agency already possessed.

During the course of the scheme, the subjects defrauded the government out of $5.25 million, much of which was laundered through a series of structured transactions or used to purchase luxury vehicles, homes, clothing, and jewelry.

Several subjects agreed to serve as cooperating witnesses in order to avoid prosecution, while the primary subject was arrested and prosecuted for various bribery, tampering, misconduct and money laundering crimes.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI investigators initiated a criminal investigation after discovering what appeared to be a large-scale extortion scheme during a review of sensitive financial information. During this review of financial data, officials identified approximately $1.5 million in cashier's checks payable to a single individual, who was subsequently negotiating the checks for a combination of cash and new cashier's checks. The subject would then continue this negotiating method until all of the cashier's checks were depleted and then use the cash to purchase vehicles, boats, and other personal expenditures.

Based on the analysis of the sensitive financial information, IRS-CI officials were able to obtain a search and seizure warrant on the subject's primary residence and discovered the source of the funds backing the cashier's checks. The primary subject had been extorting a wealthy area businessman out of $2.5 million in cash and cashier's checks with the threat of violence and police involvement over a relationship the businessman allegedly had with a relative of the primary subject and alleged criminal misconduct of the businessman. This information led to additional search and seizure warrants, resulting in the seizure of 17 vehicles, motorcycles, boats, and jet skis. The seizures led investigators to several family members of the primary subject, who each gave conflicting stories and made threats to other witnesses in an attempt to obstruct the investigation.

The primary subject of this investigation and several family members were named in a 119 count indictment. These individuals were arrested and pled guilty to money laundering and tax evasion charges. One subject died of a drug overdose before sentencing, but the others were sentenced to 60 months in prison and 2 years' supervised release.

Immigration and Customs Enforcement (ICE-HSI)

HSI officials analyzed an enormous volume of sensitive financial information to target a Florida-based criminal operation hiring, harboring, and exploiting undocumented immigrant workers. This organization utilized a network of money services businesses (MSBs) to carry out an elaborate check cashing and workmen's compensation insurance fraud scheme. Part of their scheme involved recruiting Florida DMV employees to fraudulently provide the subjects with identification information of individuals that was then used to establish multiple shell companies. These shell companies were used to carry out the insurance fraud scheme and the hiring of undocumented laborers for general contractors. Unlicensed couriers were used to conduct check cashing transactions at conspiring MSBs on behalf of the undocumented workers in return for a larger than normal transaction fee. HSI officials estimated that this organization generated in excess of $3 million in unlicensed check cashing transactions each month.

HSI investigators identified the shell companies and conspiring MSBs through analysis of sensitive financial information. This analysis led to the identification of the associated individuals and provided officials with grounds to conduct surveillance of the subjects. Initial surveillance led officials to observe an illegal check cashing transaction, leading to the arrest of several subjects for unlicensed money transmitter violations. Currency and vehicles were seized and further cooperation by one of the subjects led to the discovery and seizure of additional

fraudulent checks and over $130,000 in cash. These discoveries led to additional financial analysis, which revealed over $7.5 million in transactions conducted by this criminal organization. These transactions led to the indictment of subjects for fraud and operating as unlicensed MSBs. During the course of the investigation, HSI officials seized vehicles, and over $1 million in currency and checks.

Immigration and Customs Enforcement (ICE-HSI)

An analysis of sensitive financial information led HSI officials to open up an investigation into a subject who appeared to be conducting a high volume of unusual wire transfer activity through her financial accounts. HSI officials were notified later by investigators from several other law enforcement and regulatory agencies of ongoing cases against the same subject due to securities fraud violations.

The joint investigative efforts of several agencies determined that the subject and one co-conspirator owned several investment companies. The subject told investigators that the funds that had been deemed suspicious were her own personal funds, and not funds provided to her by clients in the form of investments. Interviews with investors revealed that these funds were in fact provided by the investors, with the intent to be used as investments in hedge funds. The subject of the investigation however, did not invest the funds in this manner and instead invested them through her own personal account. The subject had been sending fraudulent monthly statements to investors, showing positive returns and substantial profits from their investments.

The investigative efforts of HSI officials enabled them to arrest the subject on commodities fraud and wire fraud charges, which resulted in the seizure of bank accounts valued at $367,000.

Immigration and Customs Enforcement (ICE-HSI)

A long-term investigation conducted by HSI and foreign law enforcement authorities determined that a foreign government official who had previously been convicted of corruption, bribery, treason, and mutiny had hidden millions of dollars in the United States since his conviction. This official was convicted of receiving more that $200 million in bribes from various businesses and companies while serving in his government position. He then laundered these funds through a series of shell companies, nominees, and trusts in foreign countries and the United States.

In a combined effort with officials from foreign law enforcement agencies, HSI investigators analyzed a large amount of sensitive financial information and discovered assets traceable to high-level corruption, dating back to the 1990s, including nearly $29 million that was seized from the former government official and repatriated to the foreign government.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI investigators initiated this case after identifying sensitive financial information indicating their primary suspect may have been engaged in several fraud schemes. Investigators were able to determine that the suspect was utilizing various online scams to develop relationships with victims to accumulate personal information and to open bank accounts for the suspect to move funds through.

Investigators were able to determine, based on the email activity of the suspect, that he was conspiring with hackers, creating fraudulent identification information, and carrying out schemes through email communication. This analysis ultimately led investigators to the true identity of the suspect and a high volume of fraudulently filed tax returns. Physical surveillance of the individual showed him making many suspicious cash transactions using fraudulent identification.

After sufficient evidence was collected, a criminal complaint was filed and investigators successfully obtained warrants for the suspect's arrest and a search of his residence. At the time of his arrest, the suspect had several forms of fraudulent identification on multiple mobile phones in his possession. The suspect eventually pled guilty to various fraud, identity theft, and conspiracy charges. Investigators identified hundreds of fraudulently filed tax returns, collecting millions of dollars in refunds.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI officials kicked off this investigation upon being notified by an insurance company who suspected several of its clients were victims of an investment fraud scheme. Investigators poured through volumes of sensitive financial information to determine that three insurance company clients had recently transferred their policies totaling nearly $325,000 to an asset management company without any licensing or legitimacy. Investigators discovered that a fax number on the transfer paperwork belonged to a former employee of the insurance company and believed he was recruiting former clients to invest in his fictitious asset management firm. Investigators also discovered large amounts of cash that the subject was moving in and out of casinos during this same timeframe.

IRS officials later discovered that the subject had opened multiple accounts at a single financial institution under different company names. Through these accounts, the subject received deposits of large checks from insurance companies, with memos referencing individuals other than the subject. Approximately $1 million of these funds was subsequently debited from this account through casino transactions.

A Grand Jury investigation was initiated and several additional law enforcement agencies assisted IRS investigators in identifying victims and analyzing financial data. Investigators analyzed the checks deposited into the subject's accounts and interviewed the individuals whose accounts the checks were drawn on. The victims indicated they had all purchased whole life insurance annuities from the subject's father, who was an agent for legitimate insurance companies. The subject convinced the victims to move their investments to his investment companies, which were actually nothing more than shell companies. Many of the victims unknowingly authorized the subject to transfer funds from their policies to his fictitious companies, at which point the subject used the funds, totaling over $1.5 million for personal gain.

Investigators executed several search warrants on the subject's home and office and arrested him on charges of mail fraud, wire fraud, and money laundering. The subject pleaded guilty to these charges and was sentenced to 5 years in prison and ordered to pay $1.5 million in restitution.

Internal Revenue Service-Criminal Investigation (IRS-CI)

Investigators from IRS-CI, DEA, and several state agencies targeted illicit prescription writing practices, controlled substance distribution, and money laundering as part of a task force effort. An analysis of sensitive financial information identified a subject who maintained accounts at many different banks where he conducted 700 cash deposits totaling nearly $3.8 million over a 7-year period.

As a result of this discovery, officials opened an investigation focusing solely on this individual and discovered he was the source of supply for a large-scale illegal prescription pill distribution organization. Investigators determined that the subject was a doctor who was receiving cash payments for prescriptions that the subject wrote, without proper medical practices being followed.

Based on an extensive analysis of financial documents, interviews, and surveillance, investigators from several Federal agencies obtained search warrants for the subject's residence and medical practice location, and seized multiple cash receipt journals and two cash counting machines located in a large safe. A Grand Jury returned a 29-count indictment charging the subject with various financial crimes. The subject was convicted on all 29 counts and as of September 2017, faces a prison sentence of up to 51 months.

Federal Bureau of Investigation (FBI)

FBI officials opened an investigation into the subject after discovering he accepted nearly $10 million in investment money into the accounts of his company and subsequently used the funds to pay other investors and for personal expenses as part of a Ponzi scheme. FBI investigators were able to trace the illicit use of investor funds and initiate forfeiture proceedings against the subject and his company. These forfeitures included luxury vehicles and several million dollars.

Investigators were able to obtain a confession from the subject that he was operating a Ponzi scheme using investor funds. As a result of his confession, FBI officials arrested and indicted the subject on various wire fraud and mail fraud charges. Several accounts were subsequently frozen and forfeited with balances totaling $3.5 million.

The subject pleaded guilty to the fraud charges; a money judgement of $9 million was entered against him. Sentencing is pending as of September 2017, and the restitution is anticipated to be approximately $5.5 million.

Federal Bureau of Investigation (FBI)

FBI officials began their investigation into their subject as a result of an analysis of sensitive financial information. Investigators discovered reports of their subject identifying himself as customers of various financial institutions, initiating wire transfers from their brokerage accounts into his own personal accounts. This individual had previously been fired from an investment advisory firm and had his license suspended as a result of removing funds from client accounts without authorization.

Investigators determined that the subject had obtained his clients' account login credentials and regularly wired funds from their investment accounts to his own accounts for personal gain over a period of 7 years. If questioned by clients during that time, the subject provided them with fraudulent account statements and misled them into believing he was investing the funds on their behalf. During an interview with FBI officials, the subject admitted that he never invested any of the funds and used the money for personal gain as quickly as he could steal it. Officials determined this amount to be nearly $2 million, which was used largely for cash purchases and gambling activity.

FBI officials arrested and indicted the subject on wire fraud charges, to which he pleaded guilty. He was sentenced to 75 months in prison and ordered to pay restitution of $1.8 million.