



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

Category: Third Party Money Launderers

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 “Third Party Money Launderers Threat.” 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 obtained 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 business and individuals controlling it were indicted on multiple money laundering and tax violations. The individuals operating the business both pled guilty to all charges.

Internal Revenue Service-Criminal Investigation (IRS-CI)

A multi-agency task force, led by IRS-CI investigators, identified an individual as a major distributor of methamphetamine. The organization headed by this individual obtained the methamphetamine from the west coast and distributed it throughout the United States, primarily in the Midwest. An analysis of sensitive financial information, as well as surveillance efforts of several agencies, led to the identification of the target's primary source of supply and several other associates.

Several of these associates cooperated with investigators and provided additional details on the primary target, corroborating information already obtained by investigators. This information, along with a large volume of sensitive financial information, enabled investigators to execute multiple search warrants on the homes of the primary suspects and several associates.

During the investigation, it was revealed that the primary target was laundering proceeds of methamphetamine sales through a used car dealership owned and operated by another individual. Surveillance of the primary target and this car dealership corroborated this information. The primary target used the auto dealership to launder the funds through a complex series of vehicle transactions. As a result of the financial investigation, 12 automobiles and 2 motorcycles, with a value of \$251,000 were seized from the primary target. Most of these vehicles were located on the property of the used car dealership when they were seized.

The majority of the individuals pursued in this investigation entered guilty pleas for various drug, conspiracy, and money laundering charges. Several individuals, including the operator of

the used car dealership, were found guilty on conspiracy and money laundering charges due to their roles as third-party money launderers.

Federal Bureau of Investigation (FBI)

The FBI was notified by a company that they had fallen victim to a business email compromise (BEC) scheme, resulting in the loss of approximately \$57,000. As a result of the scheme, the FBI was able to identify the recipient of the \$57,000 wire transfer. This recipient was unknowingly acting as a “money mule” and was the victim of an online romance scam. He was under the impression that the funds he was receiving were on the behalf of his online girlfriend. He cooperated with agents and provided details on where he had been directed to wire the funds to next. This information revealed the identity of the primary target of this investigation.

Analysis of a high volume of financial data identified accounts and transactions associated with their primary target that appeared to be used to facilitate money movement in not only this scheme, but other BEC schemes as well. Investigators were able to contact victims of the additional schemes, who corroborated the information uncovered in the financial data.

The financial data also revealed several additional fictitious identities the subject was using to open bank accounts and money laundering activities totaling over \$1 million. Physical surveillance of the subject enabled investigators to witness additional fraudulent transactions at bank locations and arrest the subject, who was in possession of a large amount of cash and fraudulent identification documentation and bank cards.

This individual was charged with several counts of money laundering and forgery.

Immigration and Customs Enforcement (ICE-HSI)

HSI investigators initiated a money laundering investigation targeting a group of individuals laundering money through a large-scale, international, trade-based money laundering (TBML) operation. This case led to the execution of over 100 undercover operations throughout the United States and South America.

This investigation targeted several individuals who operated front companies located in South America. These businesses arranged the purchase of narcotics proceeds from various U.S. cities at below-market value. They would then sell the narcotics cash to South American businessmen who would purchase goods in the United States and export them to other countries.

In a coordinated effort with FinCEN, investigators were able to acquire and analyze sensitive financial data to identify priority targets and further develop the financial trail.

In addition to seizing over \$18 million, investigators arrested 39 individuals on various charges of money laundering and operating unlicensed money transmitters.

Immigration and Customs Enforcement (ICE-HSI)

HSI investigators received information from a cooperating defendant regarding another individual laundering illicit funds through a hawala operation that were generated from the sale of contraband cigarettes in the New York City area. The primary target and his co-conspirators utilized a network of couriers and legitimate and illegitimate money services businesses to launder money throughout the United States before smuggling the bulk cash overseas.

Information obtained through an analysis of sensitive financial information indicated that the primary target had ties to many individuals located in the Middle East. Surveillance of the target and information provided by cooperating defendants revealed that the target was planning to personally transport bulk currency to the Middle East. Law enforcement officials subsequently detained the target while he was attempting to leave the country without declaring over \$775,000 in currency he had concealed in his baggage.

The failure to declare the transportation of funds resulted in his arrest for bulk cash smuggling. Subsequent investigation led to the target's acknowledgement of his role in the hawala operation and conspiring to transport the proceeds of contraband cigarette trafficking. The target was indicted on charges of bulk cash smuggling, conspiracy, and operating an unlicensed money transmitting business.

Immigration and Customs Enforcement (ICE-HSI)

A multi-agency investigation, led by HSI, focused on a one-branch U.S. bank that had opened hundreds of foreign correspondent accounts used by currency exchanges located in South America that had no U.S. presence or discernable business practice. Investigators determined that these currency exchanger accounts were used to facilitate third-party money laundering activity, receiving large wire transfers from South America that were rapidly disbursed through many small outgoing wire transfers to recipients in the United States. Investigators identified over \$1 billion in such transactions over a 3-year period.

An analysis of sensitive financial information identified several individuals associated with this bank who appeared to be coordinating the money laundering activities. Further analysis and interviews revealed that the bank employed little-to-no anti-money laundering (AML) measures and many of the bank's customers had been identified as suspected money launderers by several other Federal law enforcement agencies.

In a coordinated effort, investigators from several agencies executed a search warrant at the bank that resulted in the seizure of communications with South American individuals, among other valuable pieces of evidence. Interviews with employees yielded additional evidence of the bank's willful AML failures. These interviews, search warrants, analysis of sensitive financial information, and other investigative techniques determined that over \$1 billion in proceeds from criminal activity, including narcotics trafficking and various fraud schemes were laundered through this bank.

The President and CEO of this bank was held criminally liable for the Bank Secrecy Act (BSA) failures and pleaded guilty to violations of the BSA, including willful failure to maintain an effective AML program, willful failure to report suspicious activity, and aiding and abetting.

Immigration and Customs Enforcement (ICE-HSI)

HSI investigators analyzed a high volume of sensitive financial information as part of their investigation into an armored car service suspected of laundering money by importing U.S. dollars and Mexican pesos from Mexico before wiring the funds back to Mexico. The sensitive financial information was derived from a FinCEN-issued Geographic Targeting Order (GTO) requiring certain armored car services to obtain additional information regarding the originator and intended recipient of funds.

Investigators were able to determine that the business address of the company they had identified in the sensitive financial information was being used by several additional companies, all owned and operated by the same individuals. Several of these companies were registered money services businesses while the others had no apparent business activities and served only as account holders for the operators to wire millions of dollars through.

The operators of these companies admitted that most of them were shell companies used solely for the purpose of opening bank accounts to move large amounts of funds. They also admitted deceiving the banks they used to move funds to keep their accounts in good standing and avoid suspicion. As a result of the interviews and analysis of financial data, investigators were able to issue Grand Jury subpoenas at several banks used by the companies and identified transaction patterns commonly associated with money laundering. A review of transaction data identified approximately \$45 million in cash deposits, followed by wire transfers through several financial institutions before ultimately being wired to entities in Mexico.

The primary subjects of this investigation pled guilty to violations related to failing to maintain an effective anti-money laundering program and forfeited \$525,000.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI officials began their investigation into their primary subject after identifying him as a suspect in a money laundering case against several other individuals. The primary subject was accepting deposits and providing loans as an unchartered financial institution, under the guise of a charitable organization.

The case originally targeted several real estate developers suspected of laundering money on others' behalf. IRS-CI officials arranged for a cooperating witness to contact the developers and seek assistance with laundering hundreds of thousands of dollars. The developers arranged the transactions through the primary subject, directing the cooperating witness to provide checks for deposit into the unchartered financial institution. The checks were subsequently turned into cash through an account maintained at a legitimate financial institution.

By operating as an unchartered financial institution, the subject and his company negotiated thousands of transactions for over 350 individuals through a dozen different bank accounts that

he held at multiple legitimate financial institutions. Investigators determined that many of his “clients” utilized this arrangement to hide income, launder money, negotiate third-party checks, and conduct business transactions they would not be able to conduct on their own through a legitimate financial institution. These deposits totaled over \$40 million.

The primary subject of this investigation pled guilty to charges related to his operating of an unchartered financial institution and failures to file tax returns. He was sentenced to 27 months in prison and ordered to forfeit \$500,000.

U.S. Attorney’s Office – Central District of California (USAO-CDCA)

Federal officials initiated an investigation into a California casino’s operations after the discovery of sensitive financial information indicating the casino may be laundering money on behalf of others, including leaders of suspected criminal organizations.

Investigators learned that the casino had recently begun recruiting “high rollers,” including high ranking members of known criminal organizations, in an effort to increase revenue. The casino also began using the services of independent gaming “promoters,” who steered high rollers to play at this casino, arranged private, unmonitored games, and allowed their names to be used in documentation, in place of the actual players. Investigators acquired evidence, including surveillance, that showed casino staff actively assisting players in avoiding reporting requirements. This included one incident where a player won over \$1 million during a 6-week period.

The casino had a written anti-money laundering (AML) program but failures to implement it demonstrated that the program was ineffective. Interviews with casino staff confirmed that the program was ineffective and referenced policies and procedures that were never put into practice. These AML failures, along with the high-dollar gaming of members of criminal organizations, was known to the casino’s employees, managers, President, and controlling partners.

An analysis of sensitive financial information confirmed that documentation relating to transactions of criminals was filed in the name of hired casino promoters, rather than the individuals actually benefitting from the transactions. The sensitive financial information, surveillance, interviews with employees, and other investigative techniques led the casino operators to enter into a settlement agreement to sell the casino. Additionally, the operators were charged with various money laundering violations and forced to pay over \$4 million in fines and forfeitures.

Immigration and Customs Enforcement (ICE-HSI)

ICE-HSI officials initiated an investigation into potential money laundering by a money services business (MSB) agent location based on an analysis of sensitive financial information, which indicated frequent, high value, cash deposits into a single bank account. Investigators determined that over \$21 million in funds was laundered by this MSB.

In coordination with several other Federal law enforcement agencies, HSI investigators identified substantial evidence documenting long-term practices of the MSB to launder millions of dollars

to accounts held at Chinese financial institutions. As a result of this joint investigation, officials were able to obtain guilty pleas from the two principals of the MSB on various money laundering and conspiracy violations.

During the course of the investigation into this particular agent, HSI officials developed evidence indicating culpability on the part of the parent company for failing to identify the violations of their anti-money laundering (AML) policies. This investigation was joined with those of several other law enforcement agencies into similar violations by the parent company. As a result of this coordinated effort, the parent company agreed to forfeit \$586 million and enter into agreements admitting criminal violations, including failures to maintain an effective AML program, and aiding and abetting wire fraud.