UNITED STATES DEPARTMENT OF THE TREASURY
FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK
P.O. Box 39 · Vienna, VA 22183-0039 · www.fincen.gov

FinCEN news releases are available on the internet and by e-mail subscription at **www.fincen.gov**.
For more information, please contact FinCEN's Office of Public Affairs at (703) 905-3770

FOR IMMEDIATE RELEASE
May 9, 2017

CONTACT: Steve Hudak
703-905-3770

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

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) held its third annual Law Enforcement Awards ceremony today at the U.S. Department of the Treasury. FinCEN presented 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 scope and quality of the data that we are collecting through Bank Secrecy Act reporting is constantly improving, and FinCEN has made great advancements to provide law enforcement and stakeholders faster and easier access to financial intelligence that will assist with investigations and prosecutions," said Treasury Secretary Steven T. Mnuchin, who congratulated award recipients at the opening of the awards ceremony. "These success stories highlight the value of our ongoing efforts to strengthen partnerships to combat money laundering, fraud, corruption, criminal trafficking, and other illicit activities."

The program includes six award categories recognizing achievements in combatting significant threats to the integrity of the financial system and the safety of our communities. The program is open to all Federal, state, local, and tribal law enforcement agencies. The 2017 award recipients are listed below.

SAR Review Task Force: New York State Police

The New York State Police Special Investigations Unit at the Financial Crimes Unit (FCU) identified suspicious transactions occurring in the Hudson Valley Region indicative of money laundering as part of Suspicious Activity Report (SAR) review initiatives. The impetus of the investigation was a single financial institution reporting an unusual pattern of cash deposits. The reporting bank indicated that it believed much of the cash was derived from the illegal sale of

marijuana. The funds were rapidly withdrawn from ATM locations across the United States. Investigators identified many additional reports containing sensitive financial information, dating back another year, indicating similar activity in this account.

Further investigation demonstrated that these individuals were connected to a larger criminal organization than originally believed, allowing the organization to be considered an "enterprise" and eligible to be charged under the Racketeer Influenced and Corrupt Organizations Act.

Investigators discovered extensive criminal histories for many of the individuals associated with this organization, including narcotics and firearms possession charges on several individuals. The Special Investigations Unit initiated a criminal investigation, and the two parallel investigations led to the identification of expansive criminal organizations responsible for bringing large quantities of narcotics into the region, operating business fronts used to launder funds, weapons trafficking, bulk cash smuggling, and extensive gang activity, including murder. Over 100 individuals belonging to several different street and prison gangs were identified, ranging from leadership to low-level associates, along with residences and vehicles belonging to these individuals.

As a result of this multi-agency investigation, law enforcement successfully seized 16 firearms, 14 kilos of cocaine, 12 pounds of marijuana, 90 grams of crack cocaine, 153 grams of heroin, 75 oxycodone pills, $200,000 in cash, and several vehicles. Coordinated efforts resulted in the arrest and indictment of 55 individuals in the Northern and Southern Districts of New York.

Transnational Organized Crime: Federal Bureau of Investigation (FBI)

The FBI initiated an investigation after receiving a referral from local law enforcement regarding an individual suspected of carrying out various fraud and money laundering schemes. A review of sensitive financial information identified a high volume of data enabling investigators to identify 80 accounts controlled by the primary target and identify funds that appeared to be derived from criminal activity. The individual was arrested and charged with money laundering, which subsequently led to his cooperation with law enforcement.

Based on information this individual provided after agreeing to cooperate with the FBI, investigators uncovered a network of criminal actors located in the United States and Canada. Investigators then used this information to identify additional accounts and transactions involving these newly identified targets at financial institutions located throughout the United States. These financial institutions described suspected money laundering activity though a series of businesses and trust accounts located in several countries. Investigators also identified additional ongoing criminal investigations by other agencies targeting this same network of individuals.

Investigators began working closely with the other agencies to identify the full scope of this criminal organization. The information obtained during this coordination led the FBI to consider this criminal organization one of its highest priority transnational organized crime targets. Working closely with foreign and domestic law enforcement partners, investigators identified members of this criminal organization operating from all over the world. Analysis of financial

activity indicated that this organization was bringing in $100-$300 million in annual criminal proceeds in North America alone.

Authorities arrested and indicted the targets on various money laundering, fraud, and conspiracy charges. Several suspects pled guilty before their cases went to trial. Several targets went to trial, where all defendants were convicted on all counts.

Transnational Security Threats: Federal Bureau of Investigation (FBI)

The FBI used a high volume of sensitive financial information over several years during the course of its investigation into a criminal organization moving hundreds of millions of U.S. dollars to support foreign nuclear and ballistic missile programs.

This investigation identified two families engaged in criminal activities. These families each operated a network of exchange houses, precious metals companies, trading companies, and front companies throughout the Middle East to carry out financial activity for the benefit of multiple OFAC-sanctioned entities, as well as several entities with close ties to foreign military organizations.

This investigation utilized information gleaned from financial data to confirm information necessary to issue search warrants and subpoenas to multiple U.S. financial institutions. Piecing together many pieces of financial data, they determined that the targets were operating one particular exchange house for foreign remittances. This information enabled a grand jury to issue more than 100 subpoenas to U.S. financial institutions relating to more than 300 targets. These subpoenas identified millions of transactions totaling over $200 billion.

During the FBI investigation, foreign authorities took legal action against several of the targets, who were arrested on a range of charges, including billions of dollars in bribery, corruption, and embezzlement. While most of these charges were ultimately dropped, the FBI was able to compare data about the foreign law enforcement investigation with evidence it had obtained through its own investigation and determined that many significant elements of the foreign investigation supported conclusions the FBI had drawn based on email, bank, and other data. As a result of the publicity generated by the foreign investigation, law enforcement gathered additional and previously unknown details on the identified individual targets and their hundreds of associated shell companies. This allowed the FBI to expand its search and more completely map out the criminal network and its funding mechanisms.

The investigation ultimately led to criminal charges of conspiracy to commit money laundering, bank fraud, and sanctions violations through two separate indictments against nine individuals, including an officer of a foreign bank. Prosecution of these individuals is still pending. Criminal forfeiture totals are expected to reach hundreds of millions of dollars.

Cyber Threats: Internal Revenue Service-Criminal Investigation (IRS-CI)

A multi-year, multi-agency investigation, led by IRS-CI focused on several targets selling narcotics on the dark web and distributing them throughout the United States through the U.S.

Postal Service. The primary targets of this investigation conducted their online activity through The Onion Router (TOR), which provided them with encryption and decryption of peer-to-peer connections. This method provided the targets with access to several dark web sites, on which they sold methamphetamine and marijuana.

The targets disguised their shipments of narcotics through the Postal Service inside packages filled with markers and drawing paper. Despite the targets' use of multiple return addresses and sender names, Postal inspectors were able to determine that the suspected narcotics mailings were originating from the same individuals based on several telling packaging characteristics.

Investigators intercepted multiple packages as a result of search warrants. Investigators were then able to determine through internet service provider records that the username associated with several undercover purchases on the dark web belonged to the same individual sending the narcotics through the Postal Service. Investigators determined that over a 6-month period, this individual sent 435 suspicious packages on at least 50 different occasions.

Sensitive financial information identified during the course of this investigation detailed specific information that corroborated the financial and personal information of the subjects of the investigation. The data also indicated that the subjects were using Bitcoins in an effort to conceal their illicit proceeds. The information identified in the financial data and from subpoenas issued to numerous financial institutions and Bitcoin exchangers helped clarify the convoluted series of transactions conducted to launder the funds.

The targets only accepted payment for the narcotics in the form of Bitcoin. The Bitcoins were then sent through a Bitcoin "blender" to conceal their source. The Bitcoins would then be redistributed back to the targets through several Bitcoin exchangers before being converted into U.S. dollars and deposited into several bank accounts.

The targets of this investigation were arrested on various drug charges, at which point several search warrants were issued on several locations where methamphetamine, marijuana, and numerous firearms were discovered. The targets were subsequently indicted and pled guilty to various drug and money laundering charges. This is notable since this is the first case in this particular Midwest district where money laundering charges were approved based on Bitcoin transactions.

Significant Fraud: Defense Criminal Investigative Service (DCIS)

DCIS initiated a long-term investigation based on structuring and excessive credit card charges identified by multiple financial institutions on a single individual. Two different working groups identified the transaction data and referred it for further investigation. Investigators determined that one of the subjects was transferring funds to a company providing subcontractor support for a military contract in Afghanistan. Further investigation determined that the company receiving the funds was a shell company owned by a U.S. military official to conceal bribery payments he was receiving in exchange for helping the primary target win contracts.

Further financial analysis identified $24 million in transactions in the personal accounts of the primary target. The majority of the transactions were multi-million dollar deposits from his employer, which was a DOD prime contractor providing logistical support and training to foreign military units. These deposits were followed immediately by transfers to several bank accounts and structured cash withdrawals.

A detailed analysis of sensitive financial information and contract documents revealed that the U.S. military official received bribes from the primary target in exchange for sensitive bidding data, including bid amounts of competitors and actual government estimates. The official was also responsible for establishing those estimates and assembling the team responsible for reviewing bids. In return for his assistance in winning $54 million in bids, the primary target paid the official over $9 million through an extensive network of shell companies and bank accounts.

The targets of this investigation eventually pled guilty to various conspiracy, money laundering, obstruction, and fraud charges. Investigators seized $12.3 million in assets from the primary target and his employer and the military official, including real property, vehicles, boats, aircrafts, firearms, gold coins, and bank accounts.

Third-Party Money Launderers: Immigration and Customs Enforcement Homeland Security Investigations (HSI)

Over the course of 18 months, HSI investigators utilized an extensive volume of sensitive financial information to assist in their investigation into a large-scale illegal third-party money laundering organization. The investigation began based largely on information gleaned from a FinCEN-issued Geographic Targeting Order (GTO). This GTO required armored car services importing or exporting funds through two specific geographies in the southwest border region to acquire additional identifying information on certain transactions.

The information that investigators discovered as a result of the GTO led them to focus on one particular armored car company that appeared to be facilitating a money laundering scheme outside southern California. Investigators discovered that the company was importing U.S. dollars and Mexican pesos from casas de cambio in Mexico and depositing them into shell company bank accounts that were opened and operated by the two individuals who owned and operated the company.

Law enforcement was able to identify and connect an address for the armored car company that was shared by several other companies owned by the same individuals. Two of these newly identified companies were registered as money services businesses (MSB). Further investigation and a detailed analysis of financial data indicated that these additional companies were simply shell companies that the two individuals used to funnel millions of U.S. dollars back into Mexico.

Subpoenas were issued to the banks used by each of these companies, as well as to all of the people known to be involved with the companies. Transaction records identified cash deposits

of $45 million over a 15-month period, which were then transferred in and out of the accounts of the various companies owned by the individuals before ultimately being wired to Mexico.

As a result of the investigation and discovery of the money laundering scheme, both individuals pled guilty to violations regarding failures to maintain an effective anti-money laundering program. They also lost all licenses necessary to operate as an MSB and forfeited hundreds of thousands of U.S. dollars and Mexican pesos.

UPDATE [1/11/18]: Click on the links below to view the other nominations for each category.

- Third Party Money Launderers
- Transnational Organized Crime
- Transnational Security Threats
- Cyber Threats
- Significant Fraud
- SAR Review Task Force

###

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.