FOR IMMEDIATE RELEASE
May 12, 2015

CONTACT: Steve Hudak
703-905-3770

FinCEN Recognizes High-Impact Law Enforcement Cases Furthered through Financial Institution Reporting

First-Ever Awards Ceremony Promotes Feedback to Industry

Washington, DC – The Financial Crimes Enforcement Network (FinCEN) today presented its first-ever Law Enforcement Awards in a ceremony at the U.S. Department of the Treasury. These awards are presented to law enforcement agencies that use Bank Secrecy Act (BSA) reporting in their criminal investigations. There are two primary goals of the program. First, to recognize law enforcement agencies who made effective use of BSA data to obtain a successful prosecution. And, second, to provide concrete evidence of the value of BSA data to the financial industry.

“It is fitting that these awards are being presented during National Police Week,” noted FinCEN Director Jennifer Shasky Calvery. “This tribute to law enforcement recognizes their exemplary achievements, and also provides additional feedback to the financial industry on how the information they provided helped the cases. For twenty five years, FinCEN has served as the bridge between the financial industry and law enforcement, and we need to let more people know about how vitally important that partnership has become.” Director Calvery’s remarks at the awards ceremony can be found here.

The awards program includes six award categories recognizing achievements in combatting five significant threats to the integrity of the financial system and the safety of our communities, plus an award for a case originating from a suspicious activity report (SAR) Review Team or task force. The program is open to all Federal, state, local, and tribal law enforcement agencies. The award recipients are as follows:

1. SAR Review/Task Force Category

Honoree: The Boston Police Department
BSA data provided the leads that helped the Boston BSA Financial Review Task Force, hosted by the IRS, identify a multi-million dollar Ponzi scheme - the largest Ponzi scheme in that city since the days of the infamous Charles Ponzi. The BSA reporting that started it all was of relatively low dollar amount. But local law enforcement, recognizing the threat to the community, seized on the information provided in the BSA reporting and acted to prevent further losses. And a further review of BSA filings revealed additional instances of possible structuring, money laundering, and other suspicious activities. At least 42 victims lost more than $10 million through this scheme. In one of the most significant aspects of this case, prosecutors indicted the defendants before any victims realized that they had been duped. In addition, this case is the first instance where prosecutors used a recently enacted state money laundering statute to seize funds in bank accounts. The defendants claimed to be working with real estate developers who had trouble getting conventional loans, and victims were promised returns of 8 percent interest. However, the defendants used the investment money for living a lavish lifestyle and gambling. The owner of the financial company operating this scheme was sentenced to serve 10-12 years; the defendant’s spouse was sentenced to serve 2 years; and the defendant’s son was sentenced to serve 2 years. This case demonstrates that all BSA reporting has value, no matter the dollar amount involved.

2. Third Party Money Launderers Category


This BSA case underscores how shell corporations can be exploited to move ill-gotten gains. Utilizing financial analysis of BSA data and undercover operations, the NY El Dorado Task Force (EDTF) successfully dismantled a highly sophisticated transnational money laundering and healthcare fraud organization that utilized a complicit money services business (MSB), multiple shell corporations, U.S. bank accounts of former J-1 visa holders, and attorneys to defraud government agencies and healthcare issuers of tens of millions of dollars. BSA records provided important leads and clues for investigators. For instance, BSA reporting on the suspects identified a series of suspicious transactions involving multiple businesses writing checks to each other, noting the signers all had recently issued SSNs, and that the businesses were listed at the same address, a residence. Other BSA reporting falsely listed participants in financial transactions who, in fact, had nothing to do with the transaction. By identifying attempted deception, this reporting is also valuable. EDTF identified the MSB, approximately 30 shell companies, and a large network of healthcare clinics and durable medical equipment suppliers. The scheme included the use of fraudulent billing companies to file no-fault accident claims with insurance companies on behalf of medical clinics and equipment providers. Upon receipt of payment from the insurance companies in settlement of the claims, the conspirators drew checks payable to a complex web of shell companies. These shell companies appeared to be healthcare related, but in fact did no legitimate business and were incorporated in the names of long-departed foreign students who had received special short-term visas to study in the United States. The investigation yielded 7 criminal arrests, 13 indictments, 9 convictions, and the forfeiture of approximately $3.4 million in U.S. currency.
3. Transnational Organized Crime Category

Honoree: Los Angeles High Intensity Drug Trafficking Area (HIDTA), Internal Revenue Service-Criminal Investigation, Drug Enforcement Agency, and HSI

The case, initiated by the Southern California Drug Task Force High Intensity Drug Trafficking Area (HIDTA), began as the result of BSA reporting filed by an alert financial institution and targeted an international money laundering operation involving a Black Market Peso Exchange (BMPE) scheme. During the course of this investigation, BSA data tied financial activities to the subjects of the investigation. Analysis of BSA filings by the case agent indicated the company’s bank account received structured cash deposits in locations where the business did not have any customers. This case resulted in the first BMPE money laundering conviction in the Central District of California. It involved the convictions of multiple customers using the BMPE scheme, operating an unlicensed money transmitting business, and evading financial reporting requirements. It was transnational and touched illegal activity by the Sinaloa Cartel and money launderers in Colombia. This case was also the impetus for another BMPE investigation targeting the garment district in Los Angeles which resulted in the seizures of narcotics and over $100 million in cash during September 2014. While there were many investigative tools used during the course of the investigation, BSA data strongly supported the successful prosecutions of the subjects in this case. In the end, nine individuals ended up pleading guilty to various money laundering related charges.

4. Cyber Threats Category

Honoree: HSI, New York

HSI-NY, El Dorado Task Force (EDTF) joined an ongoing investigation into Liberty Reserve, a Costa Rican company that offered digital currency. Dozens of BSA records filed by more than 20 financial institutions described staggering amounts of funds transfers, helping complete the puzzle for investigators. Liberty Reserve facilitated international crime by providing anonymity to individuals involved in illicit financial transactions. It allowed criminals to use its currency to make and receive payments for illicit material or activity including child pornography, Ponzi schemes, stolen identity, credit information, narcotics, and other contraband. Liberty Reserve was specifically designed and frequently used to facilitate money laundering in cyber space. It is estimated that $6 billion Liberty Reserve dollars were processed within this platform from 2009 thru 2013. In May 2013, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern. This was the first use of such authorities by FinCEN against a virtual currency provider. Liberty Reserve and its operators held millions of dollars in bank accounts worldwide. Pursuant to seizure warrants and restraining orders, U.S. authorities have frozen a total of approximately $40 million.

5. Significant Fraud Category

Honoree: U.S. Naval Criminal Investigative Service (NCIS)
It was only with the help of BSA information that this investigation by the Naval Criminal Investigative Service unearthed a significant bribery scam involving several co-conspirators and millions of taxpayer dollars. This contracting fraud scheme began when a program officer solicited a bribe under the threat of discontinuing Government contracts. Through the 15-year scheme, thousands lost jobs and several million dollars was stolen from the U.S. Government. In 14 months alone, more than $281,000 in suspect funds was transferred into the suspect’s account. The investigation was stalled for several years until a single BSA document was identified by investigators tied to suspicious activity of one of the subjects of the investigation. The defendants were convicted on bribery related charges, and joint restitution to the government amounted to almost $20 million. Without critical BSA data, this devastating scheme could have perpetuated for much longer, with even greater damage.

6. Transnational Security Threats Category

Honoree: United States Attorney’s Office, Southern District of Florida

This case out of the United States Attorney’s Office for the Southern District of Florida exemplifies how BSA data can intersect with other criminal investigative techniques to paint a full picture of terrorism material support and other threat finance crimes. The case originated in 2008 with BSA data concerning an individual who was later convicted of conspiring to provide and providing material support to the Pakistani Taliban. The defendant funneled money to Pakistan as Taliban insurgents fought for greater control in northwest Pakistan. BSA data was critical in uncovering the diverse and complex methods the individual used to send money from the United States to Pakistan, each of which was designed to conceal and support his activities. Investigators uncovered at least three methods: 1) wire transfers from the United States to Pakistan, where an associate picked up and administered the funds; 2) transfers of funds from cashier’s checks drawn on U.S. banks to a bank in Pakistan where co-conspirators could draw checks; and 3) bulk cash carried by family members and other travelers from the United States to Pakistan. SAR narratives helped explain how funds traveled from the United States to areas of Pakistan. The timing of this case proved extremely helpful in the fight against the Pakistan Taliban as important information gleaned from BSA records proved critical in obtaining other leads. The data led to subpoenas for bank and financial records (admissible evidence), alerted investigators to the use of wire transfers, and revealed the centrality of specific bank accounts to the scheme. This case demonstrates that BSA data, when taken with other resources at the disposal of law enforcement, can effectively disrupt terrorism support networks and mitigate other threats to public safety.

###

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.