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 10, 2016

CONTACT: Steve Hudak
703-905-3770

FinCEN Awards Recognize Partnership Between Law Enforcement and Financial Institutions to Fight Financial Crime

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today presented its second annual 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 reporting provided by financial institutions in their criminal investigations. There are two primary goals of the program. First, to recognize law enforcement agencies which made effective use of financial institution reporting to obtain a successful prosecution. And, second, to demonstrate to the financial industry the value of their reporting to law enforcement. The industry's continued commitment to provide prompt and accurate reporting is vital to the successful partnership with law enforcement to fight financial crime.

"Without the valuable information that U.S. financial institutions provide, the significant cases recognized here today would likely never have seen the light of day," noted FinCEN Director Jennifer Shasky Calvery. "These awards represent a small sample of the work that goes on every day, across our country and with international partners across the world, to fight financial crime and terrorist finance. FinCEN is proud to act as the bridge between law enforcement and the financial industry, and we will continue to recognize and promote this important partnership."

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 award recipients are as follows:

SAR Review Task Force: Internal Revenue Service-Criminal Investigation (IRS-CI)

A significant fraud investigation was initiated following a review of financial institution reporting by a SAR review team and related financial task force. Both suspicious activity reports (SARs) and currency transaction reports (CTRs) were essential in uncovering a scheme where a financial advisor depleted all of the financial resources of an impaired adult. Several alert financial institutions filed more than two dozen reports in this case. The reporting described transactions that included excessive cash deposits, alleged misuse of a position of trust, unusual increases in cash withdrawals at multiple financial institutions, and tied the perpetrator and victim together. The information provided by banks and casinos identified specific transactions, locations related to the fraudulent activity, and how portions of fraudulently obtained funds were used.

Multiple financial institution reports identified the perpetrator as a financial advisor and noted an increase in cash transactions in his personal accounts, while others identified unusual cash withdrawals from the victim's accounts.

Investigators used the information provided by the reporting financial institutions to uncover the full magnitude of the scheme and to successfully prosecute the perpetrator. Ultimately, the perpetrator pled guilty to Federal charges of money laundering, and wire and mail fraud, and was sentenced to several years of imprisonment and ordered to pay hundreds of thousands of dollars in restitution.

Transnational Organized Crime: Federal Bureau of Investigation (FBI)

Financial institution reporting played a key role in the investigation of one of the top international proliferators for weapons of mass destruction (WMD), as well as a principal supplier to Iran's ballistic missile program.

The FBI NY Field Office (FBI NY) identified and reviewed dozens of reports provided by financial institutions against the multiple front companies that were utilized by the proliferator's network to determine if he or his companies had illegally gained access to the U.S. financial system. Based on more than 40 reports filed by numerous New York banks, FBI NY determined that the proliferation network had in fact illegally laundered millions of dollars through multiple New York banks. The information in the reports guided FBI NY's investigation and helped identify over 20 front companies and bank accounts.

FBI NY identified 165 transactions that the proliferators used to illegally funnel approximately $8.5 million dollars through the U.S. financial system. Driven by the vast amount of financial institution reporting collected and examined, multiple U.S. Government agencies, led by FBI NY, were able to take coordinated, simultaneous actions against the proliferation network. In April 2014, the Department of Justice U.S. Attorney's Office for the Southern District of New York unsealed a seven-count Federal indictment against the proliferators and seized and forfeited nearly $6.5 million from the proliferators bank accounts; Treasury's Office of Foreign Assets Control designated eight associated front companies; the Department of Commerce added nine China-based suppliers to its Entity List; and the State Department instituted a $5 million reward for information leading to the arrest of the proliferators. Harnessing the financial institution

reporting, FBI NY was able to conduct outreach to U.S. banks through FinCEN, resulting in the use of a USA PATRIOT Act provision to seize millions from the proliferators' foreign bank accounts. The seizure of the proliferators' assets, and the other coordinated enforcement actions taken, severely impacted the proliferators' ability to acquire WMD materials. This whole of government approach was a model of interagency cooperation, which is proving to be increasingly critical to successfully combating the ever-evolving and complex threats to national security posed by international proliferators.

Transnational Security Threat: U.S. Customs and Border Protection, National Targeting Center (CBP-NTC)

CBP-NTC, which identifies potential threats to U.S. security, has become even more critical because of threats posed by foreign terrorist fighters, and financial institution reporting is proving to be very valuable in their efforts.

In one example, CBP officers stationed at the NTC learned that two people were arrested during counterterrorism raids in Berlin, Germany, on charges of recruiting fighters, procuring equipment, and funding ISIL. Through interagency coordination and research of U.S. Government databases, CBP officers were able to fully identify the subjects, both of whom were known to the intelligence community, and were already listed in the FBI terrorist screening database (TSDB).

NTC officers searched reporting provided by financial institutions and identified several reports filed on one of the subjects because of suspicious money transfers in Germany. NTC's analysis showed that the subject was involved with a network of individuals transferring money between Europe and Turkey. The reporting from financial institutions further identified a total of 43 people, seven of whom were positive matches to individuals listed in the TSDB. Three of those seven also were on the TSA no-fly list as being threats to civil aviation.

Through that research, NTC found another financial institution report identifying 73 additional individuals, 23 of whom were listed in the TSDB and six of those were on the no-fly list. After coordinating with the FBI, the NTC identified yet another filing with 32 people, 22 of whom were listed in the TSDB, and two who were on the no-fly list. Further coordination with FinCEN linked one of the initial suspects to 111 people, 22 of whom are listed in the TSDB, and 10 on the no-fly list. In all, NTC submitted 85 previously unknown subjects for nomination to the TSDB and enhanced another 38 records with additional identifying information to ensure they were fully identifiable by U.S. law enforcement agencies.

Information provided by financial institutions not only confirmed a number of subjects that investigators were already looking for, but identified a significant number of new, potential threats. The NTC shares the information gathered in cases like this with its U.S. interagency partners, including the National Joint Terrorism Task Force, the National Counterterrorism Center, Homeland Security Investigations, and FinCEN for further action. Through assistance from the Department of the Treasury, NTC was able to also pass this information to foreign law

enforcement partners, who were then able to enhance their country's investigations into this network.

Third Party Money Laundering: IRS-CI

Financial institution reporting played an important role in a joint investigation by the FBI, IRS-CI, and the United States Attorney's Office for the Northern District of California, which led to the dismantling of an organized criminal enterprise that participated in bank fraud, conspiracy to operate an unlicensed wholesale distribution of drugs, and money laundering.

During the initial stage of the investigation, a confidential informant provided the government with information regarding the primary suspect, a money launderer. With this information, the agents queried a database containing financial institution reporting regarding the suspect. A dozen reports, filed by five different financial institutions, revealed a large-scale criminal enterprise operating an array of criminal activities to include the sale of diverted pharmaceuticals and money laundering. The reporting provided investigators with a detailed list of bank accounts controlled by over 30 suspected individuals who established the accounts to launder their illicit funds.

The perpetrators formed multiple shell companies, some under false identities, for the sole purpose of liquidating their drug proceeds. According to the information provided by the financial institutions, the perpetrators withdrew over $15 million in currency from one bank account over a two-year period. The financial institution reporting assisted the government's efforts to decipher the complex web of shell companies, false identities, and additional bank accounts utilized by the organization. Armed with the financial institution reporting, the team reviewed records related to more than 500 bank accounts.

During the course of the investigation, the government seized over $28.6 million in cash from multiple bank accounts used to launder drug proceeds. The financial institution reporting was pivotal in providing near real-time information to identify bank accounts and account information in order to secure the seizure. In addition to the money seizure, the government seized over $2.5 million of street-diverted pharmaceuticals. A total of 33 individuals were arrested and convicted for various crimes tied to this case.

Significant Fraud: Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI)

More than 100 SARs played a key role in a significant fraud investigation undertaken by ICE. Operation Dirty Sole concerned trade-based money laundering (TBML) and the black market peso exchange involving an El Paso based company and its owner, which engaged in a long running and large scale smuggling and mail and wire fraud scheme. The primary business of the company was to wholesale goods to Mexican and U.S. based customers.

The subjects of the investigation engaged in a scheme whereby millions of dollars' worth of goods were smuggled into Mexico in violation of U.S. laws and regulations governing exportation. The goods were smuggled after Mexican Customs officials and other Mexican government officials were bribed, allowing both the business and the purchasers to avoid paying the very high tariffs otherwise imposed on the import of these products into Mexico. Further, the goods were obtained by fraud and deceit, as the business was only authorized by its suppliers to sell the goods on a retail basis.

Initial queries of financial institution reporting revealed more than 100 SARs filed by numerous financial institutions for possible structuring and/or money laundering. These reports, along with other financial institution reporting, significantly assisted law enforcement in the investigation and prosecution of this case. For example, one notable report informed that the subject was regularly depositing cash which literally smelled laundered, as if had been cleaned with detergent. Another report concerned a key customer of the business under investigation. From this information, HSI agents in El Paso were able to connect this case to a Drug Enforcement Administration investigation in Seattle involving narcotics proceeds being deposited into bank accounts and ultimately wired to the business under investigation.

Ultimately, hundreds of relevant SARs, approximately 1,800 CTRs, 250 8300s and 100 CMIRs added value to this investigation. In all, the primary subject and business were held accountable for over $100 million in illegal proceeds.

Four individuals were successfully prosecuted and convicted in this case. The primary suspect pled guilty to the most serious offense (conspiracy to commit money laundering), and agreed to forfeit over $600,000 in U.S. dollars seized and a business building with over $200,000 in equity. He also agreed to forfeit items seized during the investigation, with an estimated value of over $1,000,000 U.S. currency. He was sentenced to more than ten years of imprisonment.

Cyber Threats: New York State Police

While reviewing financial institution reporting, a New York State Police SAR Review Team based in Albany discovered that over a six-month period a subject had conducted large, unsourced cash deposits totaling over $170,000, more than 20 of which were structured below the CTR reporting threshold. A New York State Police Financial Crimes Unit investigation revealed additional financial institution reports indicating that the subject was unemployed and was depositing cash into different bank accounts from which the money was being withdrawn, transferring cash for the purchase of virtual currency via the internet, and exchanging small denomination bills for larger denominations. The subject provided no source of income to institutions and stated he was trading Bitcoins.

An initial investigation revealed the subject was a college student who had moved over $250,000 in less than six months through two financial institutions via deposits under the CTR reporting threshold, or virtual currency purchases and sales. Additionally, the subject would only keep the bank account open for about a month or so then close the account and re-open a new account, making it appear that the subject was running an unregistered money services business. Through

cooperation with the virtual currency businesses, investigators developed a lead in an illicit Dark Web-based market used for the specific purpose of buying/selling illegal and illicit items. Specific banking transactions conducted by the subject were traced to the purchases of virtual currency and then to the Dark Web market.

The investigation then led to the school where the subject attended, and the local university police advised that the subject was possibly involved in distribution of drugs on campus. Working in cooperation with the local county drug task force, the local district attorney's office, and the county court, information was developed that the subject was running a large scale drug operation on the campus, and a financial history was developed of how the subject was purchasing drugs using Bitcoin. An undercover operation culminated in the arrest of the subject, seizure of large amounts of illegal drugs, and the maximization of forfeiture opportunities. The subject was successfully prosecuted.

###

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.