



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

### **Category: Cyber Threat**

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 “Cyber Threat.” A brief summary of each 2017 nomination within this category is provided below.

#### **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.

### **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.