Compilation of Award Recipient & Nominated Cases

Cybercrime – *Homeland Security Investigations*

Homeland Security Investigations (HSI) initiated an investigation into a transnational criminal organization (TCO) involved in the production and distribution of child sexual exploitation material (CSAM). Investigators utilized Bank Secrecy Act (BSA) reporting to query a subject believed to be the owner of several websites containing CSAM along with associated businesses. Through BSA reporting, law enforcement not only found critical information on their primary subject but they also were able to identify additional members of the criminal organization and expand the investigation.

Investigators also utilized the 314(a) and Egmont Programs to assist with the investigation. The results of their 314(a) request yielded several bank accounts that were previously unknown. Egmont requests were sent to several countries and returned positive results that aided in identifying additional members of the TCO who acted as photographers and recruiters of the child-victims.

Law enforcement executed simultaneous Federal search warrants in the United States and coordinated a seizure of computer servers controlled by the TCO in a foreign country. The co-conspirators were indicted on conspiracy to commit money laundering and subsequently arrested.

Homeland Security investigators were present in a country in southeastern Europe when another subject was interviewed and four locations were searched for evidence of their involvement in the TCO. The subject was subsequently indicted, arrested and detained on conspiracy to advertise and distribute visual depictions of minors engaged in sexually explicit conduct.

The primary subject was sentenced to 63 months incarceration, another to 151 months, and a third to 144 months. The U.S. Attorney's Office, Middle District of Florida prosecuted this case.

Transnational Criminal Organization Activity – *Drug Enforcement Administration*

The Drug Enforcement Administration (DEA) initiated an investigation into a large-scale drug trafficking and money laundering organization based on a lead received from the Internal Revenue Service - Criminal Investigation. In furtherance of this investigation, law enforcement reviewed over 1,950 Bank Secrecy Act (BSA) records.

Focusing on patterned BSA filings, investigators were able to identify over 200 individual remitters, operating in multiple regional cells, who were all purchasing official checks found to be sourced with illicit drug proceeds. These ongoing financial leads enabled law enforcement to target specific remitters, as well as recipients.

As this case and financial leads developed, law enforcement was able to identify the head of the criminal organization who was responsible for laundering millions of dollars in narcotics proceeds on behalf of the organization through regional cells throughout the Eastern and Western Hemispheres. This international criminal syndicate consisted of actors from many specialized fields to include accountants, attorneys, notaries, bankers, real estate brokers, high-level corrupt government officials, and numerous lower level workers. Associates of the primary suspect routinely engaged as operators of unlicensed money remitters.

Through various investigative techniques, law enforcement was able to identify bank accounts, businesses, and additional members of the organization. In September 2020, the primary subject was extradited from a military base in Latin America to the United States.

This investigation has led to 23 arrests, the seizure of approximately 804 kilograms of cocaine, and approximately $8,225,568 USD in narcotics proceeds.

Additionally, through coordination with DEA in various locations, investigators were able to identify an ancillary organization for which the same subject laundered millions in drug proceeds. In that collateral investigation, agents have seized $9,649,903 USD with another $40 million USD in seized real estate, 1.2 metric tons of cocaine, and 98 arrests.

To date as a direct result of this investigation, law enforcement has seized approximately $17 million USD, $40 million in real estate assets, an excess of 1.2 metric tons of cocaine, and executed 121 arrests.

The U.S. Attorney's Office, District of New Jersey prosecuted this case.

Drug Trafficking Organization Activity – *Kansas City Police Department*

Through information received as a result of an interdiction stop, the Kansas City, Missouri Police Department (KCPD) was able to identify a high-tiered illegal controlled substance distributor and money-laundering target. The subject of the stop was indicted on drug charges. A search of Bank Secrecy Act (BSA) data on the subject revealed financial transactional data similar to a money/drug courier between the Midwest and the West Coast. The arrest and indictment of the driver was significant as it prompted the distributor to find a new driver to continue their marijuana and money laundering activities.

A detailed search of multiple BSA reports related to the primary target identified other members of the Drug Trafficking Organization (DTO) as well as the various methods used to move the illicit proceeds◎bulk cash smuggling, peer-to-peer applications, and wire services. Additionally, investigators utilized the 314(a) Program to identify any unknown money laundering methods for other members of the DTO.

Through various investigative techniques, law enforcement was able to identify the core network involved in marijuana distribution for the organization. During a related traffic stop, $665,000 was located during a search of the vehicle.

Through the course of the investigation, a strong work relationship developed between investigators and the financial institution of the subject. Based on information provided by the financial institution, law enforcement was able to execute a search warrant on the primary subject's residence that resulted in the seizure of multiple weapons, marijuana, multiple cell phones, high-end jewelry, money order receipts, drug ledgers, and approximately $1,638,980 USD. In addition, search warrants were obtained for safe deposit boxes used by the subject and resulted in locating $539,000 USD.

As part of the ongoing Organized Crime Drug Enforcement Task Forces (OCDETF) investigation, law enforcement federally indicted 10 members of the target organization. This DTO was identified as supplying multiple smaller drug trafficking organizations in the area and was linked to multiple acts of violence.

Following the execution of a search warrant involving members of the organization, law enforcement seized approximately $3,582,980.

Following the arrests of the indicted suspects, law enforcement executed four Federal search warrants. As a result, the following was seized: $567,309 in U.S. currency, 10 assault rifles and pistols, 72 pounds of marijuana, 36 grams of cocaine, a marijuana grow operation, 8 pounds of edible marijuana, and roughly $400,000 of seized jewelry and vehicles. In total, this OCDETF investigation resulted in the seizure of $4,150,289 in U.S. currency. The Kansas City Police Department used BSA data to drive the investigation and assisted in the largest U.S. bulk currency seizure in the Western District of Missouri.

During the course of the initial investigation, law enforcement was able to identify a target who was creating fictitious employment verification documents, including paystubs, and providing these to individuals under court supervision for a fee. In addition, the subject sold fraudulent documents and identifications including fraudulent state driver's licenses to individuals. The individuals who possessed these documents utilized them to rent apartments, houses, and warehouses to further commit criminal activity under fictitious names and companies. The subject was charged in a five-count indictment by a Federal grand jury.

The U.S. Attorney's Office, Western District of Missouri prosecuted both cases.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations (HSI) was contacted by a state's Department of Banking regarding a licensed money services business (MSB). The MSB was identified as being involved in business practices and relationships outside the scope of its MSB license. During annual audits, the state banking regulator identified numerous irregularities to include undisclosed domestic bank accounts, customers conducting business in unlicensed states, financial transactions with no apparent purpose and other transactions that appeared be indicative of money laundering.

During the investigation, law enforcement determined that the MSB remitted more than $167 million to include more than $160 million to bank accounts in a West African country. Though only licensed to remit money in certain states within the United States, the MSB remitted money on behalf of tens

of thousands of customers from nearly every state in the country. Law enforcement identified dozens of its customers that had received proceeds of various frauds and swindles, and then used the MSB as a conduit to remit money to the West African country.

Investigators confirmed the MSB was operating well outside of its purported business model and effectively had no anti-money laundering program. The business would grossly under-report actual remissions for certain customers, many that were linked to fraud, in some instances by more than 90 percent. Analysis of records provided by the MSB to state regulators and financial institutions resulted in irregularities to include little or no vetting of customers, a massive under-reporting of overall remission activity, undisclosed relationships with several banks and undisclosed relationships with other MSBs.

Numerous customers of the MSB have been arrested by state and Federal law enforcement for various offenses to include wire fraud and money laundering. A Federal grand jury indicted the MSB, along with its owners, and several other co-conspirators. Seizures associated with this investigation total more than $3 million. Over 1,900 Bank Secrecy Act filings assisted law enforcement with this successful investigation. The U.S. Attorney's Office, Northern District of Texas prosecuted this case.

Proliferation Financing – *Federal Bureau of Investigation*

The Federal Bureau of Investigation initiated an investigation into a long-running scheme by a telecommunications company, its chief financial officer, and other employees deceiving numerous global financial institutions and the U.S. Government regarding its business activities in Iran.

Bank Secrecy Act (BSA) reporting was critical to the execution of this investigation as it provided information related to the movement of illicit funds indicative of money laundering activity and IEEPA violations. The information identified specific persons of interest, targets, and subjects along with invaluable personally identifiable information for investigative leads and intelligence analysis.

The employees misrepresented the company's relationship to an unofficial subsidiary in Iran, and as a result falsely claimed the company had only limited operations in Iran and did not violate U.S. or other laws or regulations related to Iran. Through the investigation, it was discovered that the company had a longstanding Iranian subsidiary that was conducting approximately $100 million worth of U.S. dollar transactions at least some of which supported its work in Iran in violation of U.S. law, including $7.5 million for Iran-based contractors performing work in Iran.

The subject was charged with International Emergency Economic Powers Act (IEEPA) violations, intellectual property theft, obstruction of justice, bank fraud, and other crimes. The U.S. Attorney's Office, Eastern District of New York prosecuted the case.

NOMINATED CASES

Fraud – *Commonwealth of Massachusetts Office of the Attorney General*

A single Bank Secrecy Act (BSA) report initiated an investigation by the Massachusetts Office of the Attorney General's Financial Investigations and White Collar and Public Integrity Divisions into potential embezzlement by an employee at a nursing facility. The report noted that in one year, the employee had deposited over $196,000 into their personal bank account, and that these deposits were separate from the payroll direct deposits they were receiving from their employer. Review of the supporting documents related to the transactions confirmed the employee appeared to be embezzling the funds from the nursing facility by writing numerous non-payroll checks to their name and depositing them into their personal account.

As a result of the information contained in this single BSA report along with its supporting documentation, the investigative team at the Massachusetts Attorney General's Office was able to confirm the embezzlement scheme and, in turn, quickly notify the nursing facility leadership, and the employee was promptly terminated.

The subject worked for the facility for approximately nine years. When they were promoted to the position of business office manager for the entire facility, they began the ongoing criminal scheme through which they exploited their position of trust in order to access and misappropriate funds from multiple bank accounts, a corporate credit card, and the money of a resident who passed away.

The subject admitted to stealing approximately $200,000, the amount of money that was known at the time of their termination. The Massachusetts Attorney General's Office investigation later determined that the total value of the subject's theft over the course of nearly three years was over $535,000.

It is the belief of the nursing facility staff that if the Massachusetts Attorney General's Office had not notified them of the embezzlement at that time and the theft had continued, the facility quite possibly could have gone out of business due to the enormous financial loss they suffered.

The subject was sentenced to 18 months in prison, followed by nine months on house arrest, five years of probation, and was ordered to pay restitution. The case was both investigated and prosecuted by the Massachusetts Office of the Attorney General and the Massachusetts State Police.

Fraud – *New York County District Attorney's Office*

The New York County District Attorney's Office (DANY) initiated an investigation of a New York-based investment manager, and several funds and entities under his ownership and control.

During the course of DANY's investigation, the team discovered that the subject applied for Paycheck Protection Program (PPP) loans on behalf of his hedge fund, materially misrepresented his businesses' industries to financial institutions and the Small Business Administration, and provided fraudulent information on loan applications along with forged supporting documentation.

Using information contained in Bank Secrecy Act reporting, law enforcement was able to trace the flow of the misappropriated PPP funds and ultimately uncover the extent of the subject's multi-million dollar larceny from the Federal Government.

In total, the subject sought over $6.8 million in PPP loan disbursements and fraudulently obtained over $4.6 million in PPP funds.

The subject was indicted and charged with multiple felony counts and pled guilty to grand larceny, scheme to defraud, and five counts of violating the Martin Act for fraudulently obtaining over $4.6 million from the U.S. Government and multiple investors.

Fraud – *Federal Bureau of Investigation*

This investigation by the Federal Bureau of Investigation was initiated based on information contained in a single Bank Secrecy Act (BSA) filing. The information revealed multiple apparently fraudulent Paycheck Protection Program (PPP) loan applications totaling $5,202,442 submitted on behalf of 14 legal entities owned by four individuals.

Additional BSA reporting led law enforcement to quickly identify a complex loan fraud scheme. All combined, the loan amounts totaled almost $9 million, of which the subjects received over $3 million.

To date, the FBI has seized $1.2 million of the received funds.

Law enforcement executed search warrants at the subjects' residences, recovering over $100,000 in cash. One subject pled guilty and was charged with conspiracy to commit bank fraud. The U.S. Attorney's Office, Eastern District of Virginia prosecuted the case.

Fraud – *U.S. Secret Service*

This investigation, conducted by the U.S. Secret Service with assistance from the U.S. Drug Enforcement Administration and local law enforcement, revealed a physician involved in a money laundering scheme. During the investigation, law enforcement determined that the suspect used rented office space to conduct the operation of a pill mill that they opened in June 2018.

The subject quickly began to exploit the growing trend of doctor shopping and prescription fraud after another local pill mill was shut down in 2017. The suspect began to cater to those seeking drugs and illegally sold prescriptions for cash ranging from $400 to $500 each. The investigation uncovered that the doctor was using multiple accounts at various financial institutions to launder his cash proceeds.

Through the Bank Secrecy Act (BSA) data, investigators located several filings related to potential fraud and structuring committed by the subject. Numerous financial institutions identified excessive amounts of cash deposits and potential money laundering occurring within short periods.

BSA reporting was instrumental at every stage of this investigation. Well-detailed reporting by the financial institutions was instrumental in piecing together the investigative details that assisted with defining the scope of the criminal activity.

The overall investigation and financial analysis found that approximately $1,130,411 in cash deposits was structured into separate bank accounts between June 2018 and September 2020.

The subject was sentenced to three years in Federal prison for dispensing controlled substances

for no legitimate medical purpose. The court also ordered the subject to forfeit several luxury vehicles, and over $400,000. The prosecution and forfeiture were handled by the U.S. Attorney's Office for the Middle District of Florida.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations initiated a joint investigation into a group of individuals known to commit financial fraud, primarily what is known as card cracking and other criminal activity including firearms violations and the illegal use and sale of narcotics. The investigation found the individuals were collectively tied to various gangs and had substantial criminal histories involving firearms, narcotics, and fraud schemes.

Card cracking is a form of fraud where participants respond to an online solicitation for easy money and provide their bank information to include debit card, PIN, and online login credentials in exchange for cash. This information is then utilized to deposit counterfeit checks into the participants' accounts. The funds are withdrawn before the bank identifies the checks as counterfeit, resulting in significant financial losses to the banks. Criminals will use social media platforms like Facebook, Instagram, Twitter, and newer platforms such as Telegram, to solicit potential victims or collusive account holders.

Through the use of Bank Secrecy Act (BSA) reporting, investigators were able to trace the deposits of stolen U.S. Postal Money Orders to financial transactions and withdrawals for purchases. The details identified both the victims as well as collusive account holders. Agents used these leads generated by the BSA reporting to strategically develop and pursue suspects and identify the criminal network. FinCEN analytical case support was leveraged to trace the paths of stolen money, and connect bank accounts, leads, suspects, and victims back to the suspected criminal organization.

The investigation resulted in 27 Federal arrests along with two state arrests for state financial fraud violations. One subject of this investigation, charged with illegal possession of a firearm, was a career gang member. Nearly every defendant faces Federal conspiracy to commit bank fraud charges which carry a maximum sentence of 30 years.

The dismantlement of the organization has served a multitude of bank fraud victims, including individuals, banks, and government entities, whose total losses exceed $2 million. The U.S. Attorney's Office, District of New Jersey prosecuted the case.

Fraud – *The U.S. Attorney's Office, Northern District of Florida*

The U.S. Attorney's Office, Northern District of Florida initiated an investigation when a financial institution reported a questionable Small Business Administration Paycheck Protection Program (PPP) loan application on behalf of a fictitious business that was submitted using information belonging to an elderly individual who was later discovered to be residing in an assisted living facility.

Based on the information provided in the fraudulent PPP loan application, Federal investigators used Bank Secrecy Act (BSA) reporting to uncover a web of fraud, including several other fraudulent PPP loan applications, in the names of more elderly individuals, made at various national financial institutions.

One of the victims was the subject's own elderly mother, whose identity he used to fraudulently apply for and receive Economic Injury Disaster Loan (EIDL) proceeds. Through the use of BSA reporting, the scope of the investigation expanded from just one fraudulent PPP loan application to the discovery of more than $1.5 million in fraudulent PPP loan and EIDL applications and credit card fraud committed by a single subject.

BSA reporting assisted investigators with confirming the identity of the subject and their residential address. The execution of a search warrant on the subject's residence resulted in the discovery of documents that contained the personal identification information for many elderly victims. The electronic devices obtained during the search warrant revealed emails and other files relating to the elderly victims and the fraudulent PPP loan and EIDL scheme. BSA reporting along with other information gathered during the investigation led to the discovery of a credit card fraud scheme that the target began prior to the COVID-19 pandemic.

The subject was indicted for bank fraud, making false statements to a Federally insured financial institution, aggravated identity theft, and false statements. The subject was sentenced to 17 years in prison followed by five years of supervised release. Additionally, they were ordered to pay $1,560,628 in restitution and $600,000 was forfeited to the United States.

Fraud – *Federal Bureau of Investigation*

The Federal Bureau of Investigation (FBI) initiated a case based on a single Bank Secrecy Act (BSA) filing identifying questionable trading activity among the accounts of a specific group of customers. The filing noted that on two separate occasions, shortly after the option purchases, the company publicly announced it entered into an acquisition agreement. As a result, the price of the company's stock rose dramatically and the three accounts exercised their option positions for significant gains in both instances.

Based on this information, the FBI launched a full investigation of potential securities fraud, conspiracy, and wire fraud. The agents immediately contacted the U.S. Securities and Exchange Commission (SEC) and notified it of the pending investigation. As a direct result, the SEC opened a parallel civil investigation into the fraud allegations.

Without the due diligence of the financial institution and its BSA filing, this complex $1.2 million securities fraud scheme may not have been uncovered.

All subjects were charged and found guilty of securities fraud.

One subject was sentenced to three years of probation, the first nine months of which he was required to serve in home confinement, 120 hours of community service, a forfeiture judgment of $73,244, and a fine of $15,000.

The second subject was sentenced to one day in prison, three years of supervised release, a $100,000 fine, a $200 special assessment, a forfeiture judgment of $1,198,075, and 300 hours of community service.

The third subject was sentenced to 30 days in prison, three years of supervised release, a $5,000 fine, a $200 special assessment, a forfeiture judgment of $10,000, and 225 hours of community service.

The U.S. Attorney's Office, Eastern District of Pennsylvania prosecuted the case.

Fraud – *Federal Bureau of Investigation*

The Federal Bureau of Investigation (FBI) opened a case into an investment scheme predicated upon information contained in a Bank Secrecy Act (BSA) report. The subject of interest owned an investment company that served mostly elderly clients. In addition, it was discovered that another investment company owned by the subject was established solely to carry out part of the fraud scheme.

Numerous BSA reports assisted investigators with tracing the receipt of elderly victim investor funds and the transfer of funds thereafter to attempt to conceal the fraudulent activity and the identification of assets for seizure and forfeiture for restoration to the victims. The BSA reports also provided a good historical perspective of the subject's fraudulent conduct.

The subject managed the investments of more than 40 clients when he devised two schemes to defraud them. The first scheme involved false representations made by the subject to his clients that his business was a fund that invested in private corporations and guaranteed they would earn interest between eight and nine percent per year and that the investment principal was guaranteed.

As part of the scheme, the subject persuaded certain elderly clients to withdraw funds from their investment accounts and invest in the fraudulent company.

In total, the subject caused his clients to transfer $857,000. The subject spent $300,000 of that sum for his own benefit and personal expenses.

The second scheme involved false representations made by the subject to a large U.S. insurance and financial services company related to fees from his clients. The subject was able to convince the company to transfer money from his clients' accounts to an account he controlled under the guise of fee requests. In making the fee requests, Giokas falsely and fraudulently represented that he was entitled to the requested money as investment advisory fees, even though the requested amounts greatly exceeded what he was entitled to pursuant to his fee arrangements with his clients. As a direct result of this scheme, the subject received $616,396 in excessive fees.

The total loss amount as a result of the fraudulent schemes was almost $1.5 million. If not for timely BSA reporting, the schemes would have gone undetected for an unknown period of time resulting in additional victims and increased losses.

The subject pled guilty to a wire fraud and was sentenced to 52 months in jail, three years of supervised release, restitution of over $900,000, and forfeiture of over $100,000.

Fraud – *Internal Revenue Service-Criminal Investigation*

During a coordinated monthly review of Bank Secrecy Act (BSA) data led by the Internal Revenue Service-Criminal Investigation, a BSA report was identified that opened an investigation into a large health care fraud scheme. Subsequent BSA reports were critical in identifying other potential co-conspirators as the scheme involved rapidly changing business names and bank accounts.

The subjects defrauded the North Carolina Medicaid Program of millions of dollars by submitting fraudulent reimbursement claims for services that were never provided and submitting claims that misrepresented the services provided to Medicaid beneficiaries in order

to receive greater reimbursement. Funds received from the fraudulent claims were used for personal living expenses.

The primary subject was responsible for recruiting other co-conspirators to participate in the fraudulent scheme. The subjects were able to obtain prospective patient lists containing information for Medicaid beneficiaries, some of which was used to perpetrate the fraud. As a result of the fraudulent scheme, the subjects and their co-conspirators caused more than $9.4 million in fraudulent claims to be submitted to Medicaid, resulting in approximately $6.1 million in fraudulent Medicaid payments. Two of the subjects also failed to report the proceeds as income resulting in over $1.5 million in unpaid taxes.

In total, the subjects were sentenced to 22 years and ordered to pay over $8 million in restitution to North Carolina Medicaid. The U.S. Attorney's Office, Western District of North Carolina prosecuted the case.

Fraud – *Homeland Security Investigations*

Based on a tip from a bank investigator, Homeland Security Investigations (HSI), with the assistance of the United States Postal Inspection Service and the U.S. State Department Diplomatic Security Service (DSS), initiated a large-scale investigation into a transnational criminal organization found to be responsible for more than $7 million in fraudulent losses to banks and victims.

Federal agents consulted with numerous banking institutions to identify a network of dozens of accounts opened with fraudulent passports and false identities, and the account holders utilized the assumed identities to deposit stolen checks and fund withdrawals for cash and purchases.

During the course of the investigation, investigators discovered over 570 bank accounts that were opened by members of the organization, whose members operated their scheme throughout New Jersey, Pennsylvania, Maryland, Texas, and Rhode Island. The estimated fraud loss amount to the banks was $7.4 million. HSI identified 12 members involved in this fraud scheme, one of whom was arrested in Maryland on a separate fraud investigation.

Investigators linked eight seizures containing a total of 12 counterfeit foreign passports and two counterfeit foreign driver's licenses to the organization. DSS helped in associating one additional seizure made overseas to one of the organization members in the United States.

All subjects were charged with conspiracy to commit bank fraud. Four search warrants were executed and yielded numerous counterfeit passports with corresponding U.S. visas, cell phones, bank records, ATM cards, computers, over $100,000 in cash and unused money orders, numerous identification cards and documents relating to identity theft, and recently stolen checks awaiting alteration and deposit.

The U.S. Attorney's Office, District of New Jersey prosecuted the case.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations (HSI) coordinated a global investigation into a criminal group utilizing corrupt cellular phone company employees to steal the identities of over 100 victims, swap cell phone SIM cards, and steal an estimated $75 million in cryptocurrency.

The impetus of the global investigation originated with the arrest of a subject by state police on felony charges related to identity theft and the seizure of approximately $200,000 in crypto currency. The subject outlined to law enforcement the inner workings of the criminal group that led to the investigation of the group to include connections to cases throughout North America and Europe.

A Federal Grand Jury returned the first round of indictments against key members on charges related to wire fraud, aggravated identity theft, and conspiracy. In addition, a Federal Grand Jury in the Northern District of Georgia issued indictments against additional members of the organization. Shortly thereafter, Federal law enforcement executed six residential search warrants (five domestic and one international) and arrested eight members across five time zones which resulted in the seizure of approximately $3.7 million in cryptocurrency and $20,000 in bulk currency.

This investigation spanned multiple countries and involved both U.S. and international law enforcement from all levels. Their tremendous efforts resulted in the seizure of $27 million in cryptocurrency—to include the largest cryptocurrency seizure in one country's history of $5.5 million—and the arrest of 18 members. This investigation was so innovative it has been used as a template for other agencies to investigate and prosecute similar crimes through leveraging Federal, state, and international laws to go after criminal groups operating around the world. It allowed partners in the financial and cellular phone industry to make improvements to their security systems and harden their digital infrastructure to disrupt criminals from committing this type of crime in the future.

The success of the investigation would not have been possible without partnerships with the financial community and the use of Bank Secrecy Act (BSA) reporting, both by traditional and non-traditional financial institutions. The successful prosecution of this case was the result of the efforts of the following agencies: the U.S. Attorney's Office, Eastern District of Michigan; the U.S. Attorney's Office, Northern District of Georgia; the U.S. Attorney's Office, District of Connecticut; Wayne County (MI) Prosecuting Attorney's Office; and the Santa Clara District Attorney's Office.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations (HSI) initiated an investigation into a limited liability corporation and its affiliated companies, as well as its founding/managing partner and Chief Executive Officer. The investigation revealed the firm operated a Ponzi scheme that defrauded over 100 investors for upwards of one hundred million dollars.

The subject founded cryptocurrency arbitrage funds. A cryptocurrency arbitrage fund operates by taking advantage of volatile pricing on two different exchanges by buying on one exchange and selling on another, preferably at a higher price. Information indicated that several investors requested the transfer of assets from one fund to the other.

As of September 1, 2022, the transfers have not occurred despite assurances by the subject that the transfers were in process. Typically, this indicates the assets are either highly illiquid (not easily converted to cash), which would be contrary to the subject's stated trading strategy, or the assets are non-existent.

Review of multiple Bank Secrecy Act reports, along with information obtained from multiple interviews with investors, corroborated information gathered during the course of the investigation. The case resulted in one arrest and an ordered forfeiture of over $50,000. The U.S. Attorney's Office, Southern District of New York prosecuted the case.

Cybercrime – *Homeland Security Investigations*

Homeland Security Investigations conducted an investigation into a dark web narcotics vendor who was prominent on Silk Road and one of its operators. Its operator had previously been convicted on Federal charges for distributing narcotics via the Internet.

In 2018, pursuant to a judicially authorized search of the subject's house, agents found a document referring to the vendor, Silk Road, and large-scale narcotics trafficking including the deadly opioid fentanyl. Additionally, this document contained a ledger of customers whom the subject had supplied with fentanyl and pharmaceutical drugs.

In 2017 and 2018, the subject transferred bitcoin representing narcotics proceeds earned through his control of the vendor from Bitcoin addresses connected to Silk Road to an account the subject controlled at a financial institution involved in the exchange of bitcoin and other digital currency. In correspondence with that financial institution, the subject falsely claimed that the bitcoin was legitimately earned through cryptographical creation and from fair transfers with others, while the bitcoin was actually derived from Silk Road transfers. The subject converted the illegally derived bitcoin to cash worth more than $19 million.

Upon review of the transaction coupled with other related information and factors they discovered, the financial institution submitted a Bank Secrecy Act filing. This one filing led investigators to identify the account and seizing over $19 million of illicit proceeds pursuant to a judicially authorized seizure warrant.

The subject was sentenced to 42 months in prison for money laundering charges. In addition to his prison term, the subject was sentenced to three years of supervised release, ordered to forfeit approximately $19 million, and pay a fine of $10,000. The U.S. Attorney's Office, Southern District of New York prosecuted the case.

Drug Trafficking Organization Activity – *U.S. Attorney's Office, Eastern District of Arkansas*

This Organized Crime Drug Enforcement Task Force operation was led by the Bureau of Alcohol, Tobacco, Firearms, and Explosives, with substantial assistance from the United States Postal Inspection Service, the Drug Enforcement Administration, and Homeland Security Investigations. The investigation involved the trafficking of firearm parts to Mexico for manufacture into automatic weapons for drug cartels.

The investigation began when law enforcement received information regarding a shipment of counterfeit firearm parts. The parts were traced to an organization whose members were smuggling various firearm parts to ultimately be assembled into hundreds of functioning automatic weapons to be sold to and used by drug cartels.

Bank Secrecy Act reporting was invaluable in identifying members of the organization as well as describing purchases from merchants, including firearm components, ammunition, and tactical supplies. The reporting also led investigators to learn that the subject used fraudulent identities to open the vendor accounts discovered during the investigation.

Financial intelligence suggested the subjects were likely banking outside of the United States, so investigators utilized the Egmont Program. The information received from that Egmont request identified international financial accounts, many of which were fraudulently opened under fictitious identities.

Investigators executed search warrants on accounts used by the subject. Analysis of the information showed the subject was using different online identities to acquire a vast number of components for the weapons systems. It also indicated the subject was soliciting bids for others to perform machining, welding, and programing for the assembly of the firearm components in his clandestine factory.

The subject was arrested at the southern U.S. border, and admitted to ordering and receiving firearm parts from the United States and manufacturing automatic weapons in Mexico for the drug cartels.

A Federal grand jury indicted the subject and seven others for their involvement in conspiracies to traffic in counterfeit goods and to violate the Arms Export Control Act. Five codefendants have previously pleaded guilty, and one codefendant remains a fugitive. The subject pleaded guilty to conspiracy to violate the Arms Export Control Act and was sentenced to 12 years in prison.

The prosecution of this firearms trafficking organization is the first Mexican cartel firearm parts exploitation and manufacturing case in the country to be indicted and prosecuted successfully. The U.S. Attorney's Office for the Eastern District of Arkansas prosecuted the case.

Drug Trafficking Organization Activity – *Drug Enforcement Administration*

The U.S. Drug Enforcement Administration (DEA), with assistance of the U.S. Diplomatic Security Service, Homeland Security Investigations, and U.S. Customs and Border Protection - National Targeting Center initiated an investigation into a global crime syndicate led by a group of foreign nationals.

Investigators made expansive use of FinCEN's programs and resources, including Bank Secrecy Act (BSA) reporting, the 314(a) Program, the Egmont Program, and analytical support from FinCEN.

During the initial stages of this investigation, investigators were able to seize approximately 4.5 metric tons of cocaine HCL in the South American region bound for the United States. In addition to the seizures of bulk cocaine, investigators were able to assist DEA's foreign offices with the initiation of various investigative techniques that led to the arrest of foreign-based drug traffickers.

Additionally, investigators were able to successfully prevent violent criminal acts from occurring—including a kidnapping—and gained critical information into drug-related murders. The result of these efforts was two-fold: first, the investigators ultimately indicted and arrested the coordinators of these drug movements in the United States; and, second, it aided in uncovering the illicit global financial network—fueled by cocaine sales in control of the upper echelons of two brutally violent drug cartels.

In addition to the key evidence uncovering these networks, investigators also began to unravel the tentacles of the financial network supporting this group. Law enforcement discovered the network was laundering money throughout the United States and identified information related to its couriers and mid-level coordinators. Investigators used this new information to query BSA reporting on the subjects of interest and were able to uncover previously unknown information including U.S. bank accounts for a Mexico-based money launderer who was coordinating the movement of bulk drug cash throughout the world.

Partnering with law enforcement across the United States, investigators were able to seize over $1,000,000. These efforts led to the indictment of the Mexico-based money launderer, along with multiple high-level drug traffickers, the seizure of the bank accounts, and multiple arrests. Investigators further discovered extensive evidence laying out the movement of drug funds throughout the world and connecting activities occurring on the streets of a major metropolitan U.S. city with movements in bank accounts in Asia.

While searching BSA filings on one of the primary subjects, investigators were able to identify additional information leading them to the discovery of a money laundering, poly-drug trafficking, and human smuggling empire. The criminal organization was responsible for the laundering of billions of U.S. dollars, the trafficking of multi-metric ton quantities of cocaine from various countries to the United States, and smuggling foreign nationals into the United States. Following an exhaustive overseas capture operation, officials arrested and expelled the subject to the United States. Upon their arrival, they were immediately arrested by law enforcement. Within days, one of the network's principal U.S. brokers, along with a money laundering coordinator, were also arrested.

Law enforcement obtained a Federal grand jury indictment charging the primary subject with drug trafficking, multiple counts of international and domestic money laundering, bribery of a Federal official, and other identity theft related offenses, along with additional charges against three other foreign nationals. As a result of this 4-year global criminal investigation, the DEA and its global partners uncovered and ultimately dismantled a complex, worldwide enterprise responsible for laundering significant drug proceeds. The three defendants pled guilty and were subsequently sentenced to lengthy Federal prison terms.

This case was jointly prosecuted by the U.S. Attorney's Office, Eastern District of Virginia, and the U.S. Department of Justice's Money Laundering and Asset Recovery Section.

Drug Trafficking Organization Activity – *Northern Virginia Financial Initiative*

A Northern Virginia Financial Initiative (NVFI) task force officer had taken notice of a Bank Secrecy Act (BSA) report during one of their routine Bank Secrecy Act (BSA) reporting reviews. The information

reflected that the subject was transacting in unusual amounts of currency potentially related to marijuana distribution. Through further investigation into the subject, it was discovered that a nearby police department had additional information on the subject involving distribution of heroin.

Through various investigative techniques, it was revealed the subject was utilizing a stolen rental car. When canvassing the potential address for the subject, the stolen vehicle was discovered on the property. With this information, law enforcement was able to obtain and execute a search warrant of the property upon which an extensive pill manufacturing and dangerous drug distribution operation was discovered. Additional search warrants were obtained for the drug trafficking evidence. Seized and recovered as a result of those search warrants was over seven kilograms of Fentanyl (valued over $600,000), two semi-auto assault weapons, $217,955 in cash, three vehicles (valued at $56,436), jewelry (valued over $140,000), pill and kilo presses, and related paraphernalia.

As a result of this investigation, five subjects were arrested and pled guilty to conspiracy to distribute Fentanyl and were sentenced to a combined total of 564 months in prison. The U.S. Attorney's Office, Eastern District of Virginia prosecuted the case.

Drug Trafficking Organization Activity – *Drug Enforcement Administration*

The Drug Enforcement Administration (DEA), in conjunction with the U.S. Department of Health and Human Services (USHHS), the U.S. Secret Service (USSS) and the Federal Bureau of Investigation (FBI), initiated an investigation into the illicit prescribing of controlled substances by the owner and medical doctors of a pain clinic.

Law enforcement took a three-pronged approach to the investigation by conducting visits, voluntary interviews, and analysis of prescription data. The visits revealed that the facility prescribed high doses and pill counts of Oxycodone without a legitimate medical purpose and outside the course of professional practice, as demonstrated by the physicians' failure to conduct physical examinations or appropriate medical consultations of patients and the near uniformity in the physicians' prescribing practices. It was also discovered that the facility operated as an all-cash business and did not take any forms of medical insurance. Further analysis showed doctors at the facility had prescribed approximately over 1.5 million tablets of Oxycodone without medical necessity.

The initial investigation provided some information but not enough to corroborate who was benefitting from all the illicit activity and where the proceeds were being distributed. Upon reviewing relevant Bank Secrecy Act (BSA) filings, investigators were able to glean to whom and where all illicit funds were going. The extensive BSA filings led to the identification of all of the past and present major banking accounts associated with this long running enterprise. The BSA filings also revealed a number of related bank accounts that were being utilized by all involved in the conspiracy. Armed with this information, agents were able to obtain subpoenas for all related accounts. As law enforcement continued their analysis, it led to the discovery of other assets to include real property that could be directly tied to the illegal activity. The properties that were identified were all purchased by utilizing a number of limited liability corporations in an attempt to conceal the true ownership of the properties. Without the valuable BSA reporting, investigators would have had great difficulty locating the accounts utilized by the subjects.

This investigation resulted in seven arrests with all defendants pleading guilty. In addition, money judgements totaling $1,228,000 and nine pending lawsuits against properties worth approximately $3.75 million were obtained. None of these money judgements or seizures would have been possible without the BSA records, which allowed law enforcement to "follow the money." In total, to date, this investigation has resulted in the closure of a rogue large-scale pain clinic, the arrest of seven doctors and the surrender of seven DEA Registrations from medical professionals for supplying illegally diverted controlled substances. The closure of this rogue medical facility was a significant blow to the widespread opioid networks operating in south Florida.

The U.S. Attorney's Office, Southern District of Florida is responsible for prosecuting the criminal case.

Drug Trafficking Organization Activity – *U.S. Attorney's Office, Western District of Washington*

This Drug Enforcement Administration-led Organized Crime Drug Enforcement Task Forces (OCDETF) investigation dismantled a significant cross-border Drug Trafficking Organization (DTO) that used sophisticated money laundering techniques. The DTO included a compliance officer for a money services business and an unlicensed cryptocurrency exchanger. FinCEN data was instrumental in uncovering, investigating, and dismantling this DTO.

Through various investigative techniques, law enforcement was able to determine the scope of the DTO's activities to include kilograms of heroin and thousands of fentanyl-laced imitation oxycodone pills flowing into the community that generated hundreds of thousands of dollars in drug proceeds weekly.

In addition, Bank Secrecy Act filings provided investigators highly valuable insight into the DTO's modus operandi along with the bank accounts and businesses being utilized.

During the search of the primary subject's business and residence, investigators seized more than $12,000 in cash.

Agents executed nearly 90 search warrants and seized over $325,000 in cash, thousands of fentanyl-laced imitation oxycodone pills (containing at least 900 net grams of fentanyl), over 7,600 net grams of heroin, nearly 40 net grams of methamphetamine, and more than 3,000 net grams of cocaine, along with dozens of firearms. To date, 47 defendants have pleaded guilty to Federal charges as a result of this investigation, and a total of $696,149 in cash drug proceeds has been forfeited. The U.S. Attorney's Office, Western District of Washington prosecuted the case.

Transnational Criminal Organization Activity – *Homeland Security Investigations*

Homeland Security Investigations (HSI) conducted a money laundering investigation into the use of the Black-Market Peso Exchange (BMPE) by drug cartels to launder their narcotics proceeds. This case investigated the methods used by the drug trafficking organization to avoid the regulations imposed by a FinCEN Geographic Targeting Order (GTO).

Investigators became aware of numerous bank accounts whereby cash was deposited in a structured manner, appearing to avoid both the requirements of the GTO and Bank Secrecy Act (BSA) reporting requirements. The cash was deposited into accounts, and then forwarded in the form of a check or wire transfer to U.S. exporters. Hundreds of thousands of dollars were deposited into various broker-controlled accounts and then immediately converted to a check issued to a Florida exporter.

Through extensive BSA reporting, law enforcement was able to target the businesses that were recipients of the structured cash as well as wire transfers from other countries. In addition, a seizure warrant executed on one of the company's accounts resulted in the seizure of $72,281. This account was identified as receiving cash deposits in a manner consistent with the structuring of BMPE narcotics proceeds as well as wire transfers from a Mexico-based shell company. An investigation into the shell company identified numerous businesses receiving wire transfers.

A review of BSA data and other financial records identified more than $160 million in wire transfers sent to one of the businesses over a period of 18 months. Additionally, investigators uncovered more than $400,000 in money orders deposited into this account. Investigators met with prosecutors to present financial transactions involving the business and two shell companies. Based upon information derived from separate investigations, these shell companies were found to be utilized by BMPE money brokers to launder narcotics proceeds. As part of this investigation, seizure warrants were executed on U.S. correspondent banks that held a relationship with the foreign institutions domiciling the accounts of the two shell companies. In total, the analysis uncovered more than $700,000 in wires originating from these two shell entities to an account held by the business.

Charges against the business include money laundering and operating as an unlicensed money transmitter all pursuant to property derived from the sale of narcotics. The U.S. Attorney's Office, Southern District of New York prosecuted the case.

Transnational Criminal Organization Activity – *Homeland Security Investigations*

Homeland Security Investigations received information from international authorities regarding a sophisticated hacking and money laundering network operating in Europe and the United States. According to investigators, the organized criminal group was believed to perpetrate large-scale business email compromise (BEC) and other related financial fraud totaling over $10 million, the illicit proceeds of which were being laundered through shell corporations in the United States and Europe.

Throughout the investigation, investigators fully leveraged critical financial data and financial investigative techniques including significant exploitation of Bank Secrecy Act (BSA) reporting, collaboration with a Financial Crimes Enforcement Network analyst, subpoenas, and Mutual Legal Assistance Treaty (MLAT) requests. BSA data proved central to the investigation and in large part led to the identification of the network leader.

Through a comprehensive analysis of FinCEN financial intelligence, shell companies, and IP addresses, investigators were able to fully identify the leader who was a foreign national known to be a professional hacker and computer programmer. In addition, they were able to identify network associates based in the United States who appeared to be engaged in the criminal

conspiracy. Ultimately, law enforcement traced approximately $40 million associated with this network through a series of shell companies in the U.S. and overseas with an ultimate destination of a West African country.

The primary subject was extradited to an East European country—the first extradition of a foreign national to face money laundering charges in the history of this country.