Compilation of

Award Recipient & Nominated Cases

AWARD RECIPIENT

Transnational Criminal Organization Activity – *Drug Enforcement Administration*

The U.S. Drug Enforcement Administration (DEA), with assistance from 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 public-private information-sharing program FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act, cross-border information sharing via the Egmont Group of Financial Intelligence Units, and analytical support from FinCEN.

During the initial stages of this investigation, investigators were able to seize approximately 4.5 metric tons of cocaine hydrochloride in South America bound for the United States. In addition to the seizures of bulk cocaine, investigators were able to help DEA's foreign offices initiate various investigative techniques that led to the arrest of foreign-based drug traffickers. Additionally, investigators were able to successfully prevent violent criminal acts—including a kidnapping—from occurring 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, the investigation aided in uncovering an associated illicit global financial network, which was fueled by cocaine sales and under the 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 more than $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 associated 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 that led 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 the smuggling of foreign nationals into the United States. Following an exhaustive overseas capture operation, officials arrested and expelled the subject to the United States. Upon arrival in the United States, U.S. law enforcement immediately arrested the subject. 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 and multiple counts of international and domestic money laundering. Law enforcement also worked with prosecutors to levy additional charges against numerous 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. All defendants in this case have since pled guilty and have been 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.

Human Trafficking/Human Smuggling – *Department of Justice's Civil Rights Division's Criminal Section*

The Department of Labor-Wage and Hour Division launched an investigation into a subject and their company who provided foreign, non-immigrant, seasonal workers to farms in the United States. The investigators looked into whether the company was paying the required wage rate to its seasonal workers, reimbursing the workers for reasonable travel costs, and allowing workers to maintain physical control of their passports. The investigators subsequently developed evidence to demonstrate that the owner and operator of the company, along with their co-defendants, did not pay the seasonal workers the required wage rate, charged workers for their travel costs in violation of the law, and confiscated workers' passports upon their arrival in the United States. The investigative team used BSA reporting to identify financial accounts tied to the subject and their company. BSA reporting was also used to identify the criminal enterprise's financial connections to other farms. BSA reporting provided critical leads during the multi-year investigation, and several law enforcement agencies and non-profit entities worked together to bring justice to the 17 victims who cooperated with law enforcement and hundreds of other victims who were subjected to the defendants' abuse over the years.

Investigators also discovered evidence that the defendants conspired to coerce the workers into performing long hours of physically demanding farm labor for almost no pay. After charging Mexican farm workers exorbitant sums of money to come into the United States on short-term agricultural visas to work, the defendants used various coercive means to compel the victims' labor and services. These coercive tactics included imposing debts on workers; confiscating the workers' passports; subjecting workers to crowded, unsanitary, and degrading living conditions; verbally abusing and humiliating the workers; threatening workers with arrest, jailtime, and deportation;

isolating workers by preventing them from interacting with anyone other than the defendants or their employees; and threatening to physically harm the workers' family members back in Mexico if the workers failed to comply with their demands. The evidence also established that when investigators looked into the criminal enterprise's employment practices, the defendants obstructed the investigations by lying to investigators, falsifying payroll and other required records, and pressuring their workers to lie.

The level of partnership between numerous agencies in this case—to include the Federal Bureau of Investigation, Homeland Security Investigations, the Palm Beach County Sheriff's Office, the Department of Labor Office of Inspector General, the Department of Labor Wage and Hour Division, the Department of State Diplomatic Security Service, the Coalition of Immokalee Workers, Colorado Legal Services Migrant Farm Worker Division, Legal Aid Services of Oregon Farmworker Program, and Indiana Legal Services Worker Rights and Protection Project, as well as local agencies—demonstrates the investigative team's commitment to partnership and cooperation.

Ultimately, a Federal grand jury indicted five defendants. The primary subject pleaded guilty to charges of conspiracy in violation of the RICO Act and conspiracy to commit forced labor and was sentenced to 118 months of imprisonment. The other defendants pleaded guilty to RICO conspiracy and conspiring to obstruct a Federal investigation and were sentenced to a total of 78 months of imprisonment. Four of the defendants were collectively ordered to pay nearly $200,000 in mandatory restitution to 17 victims.

The U.S. Attorney's Office, Middle District of Florida and the U.S. Department of Justice's Civil Rights Division's Criminal Section prosecuted the case.

Corruption – Internal Revenue Service-*Criminal Investigation and Global Illicit Financial Team; Department of Homeland Security Homeland Security Investigations*

While working a third-party money laundering investigation, the Internal Revenue Service-Criminal Investigation and Global Illicit Financial Team identified a money remitter who was an investment advisor controlling several U.S. and foreign companies. FinCEN networking revealed that, based on BSA data, Homeland Security Investigations had also initiated an investigation on the same subject. FinCEN connected the agencies, which subsequently merged their investigations.

Between approximately 2014 and 2020, the investment advisor paid more than $2.6 million in bribes to officials of Ecuador's public police pension fund, Instituto de Seguridad Social de la Policia Nacional (ISSPOL). These bribes included at least approximately $1,397,066 to individuals who were at the time ISSPOL officials, including ISSPOL's Risk Director and a member of ISSPOL's Investment Committee to obtain and retain investment business from ISSPOL. The investment advisor allegedly obtained approximately $65 million in profits from one aspect of the scheme.

In 2021, an independent foreign investigation resulted in the arrest of four former officials from ISSPOL.

The two U.S.-based subjects pled guilty to conspiracy to launder money and were sentenced to 26 and 58 months in prison, with a forfeiture judgment of $1.4 million. One subject is currently a fugitive with extradition in process.

Agents credited FinCEN training sessions on the Real Estate Geographic Targeting Order (GTO), and the filings associated with the GTO, with helping them identify real estate the subjects purchased with illicit proceeds.

The U.S. Department of Justice Criminal Division's Fraud Section is prosecuting the criminal cases. The U.S. Attorney's Office, Southern District of Florida, is handling the asset forfeiture.

Fraud – *Internal Revenue Service-Criminal Investigation, Federal Bureau of Investigation, and Small Business Administration Office of Inspector General*

The Internal Revenue Service Criminal Investigation, Federal Bureau of Investigation, and the U.S. Small Business Administration Office of Inspector General investigated a massive pandemic relief fraud ring at the height of the COVID-19 pandemic. The investigation began shortly after the Attorney General's creation of the COVID-19 Fraud Enforcement Task Force. The team was originally tasked with investigating 10 loans made under the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020. Investigators quickly used the information found in BSA filings to identify additional fraud and linked the initial list of 10 loans to more than 150 loans totaling approximately $21 million in fraud.

Because the defendants used fictitious identities and a vast network of bank accounts to commit the fraud and launder the proceeds, investigators also used the public-private information-sharing program FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act to identify additional bank accounts for their investigation. The 314(a) program responses led investigators to additional fraud schemes and, combined with traditional law enforcement tactics, eventually led investigators to the true identity of the culprits. BSA filings were also essential in identifying relationships between co-defendants.

Prior to their sentencing, the main defendants fled the United States and became international fugitives. Again, investigators used BSA data to sniff out the financial trail. Investigators were able to run queries through FinCEN's databases and identify accounts that the suspects opened at cryptocurrency exchanges using the same fictitious identities that were used to perpetrate the original fraud. Investigators also discovered that the defendants were applying for additional loans post-indictment and even during trial. Eventually, the financial trail led investigators to discover the whereabouts of the fugitives. International cooperation resulted in extradition of the defendants.

All eight defendants have been sentenced, with the ringleaders receiving sentences of 17 years and nearly 11 years. The U.S. Attorney's Office, Central District of California, and the U.S. Department of Justice Fraud Section prosecuted this case.

Drug Trafficking Organization Activity – *Federal Bureau of Investigation*

The Federal Bureau of Investigation in collaboration with the Drug Enforcement Administration, Homeland Security Investigations, the Five Eyes Law Enforcement Group, the United Kingdom's Joint Money Laundering Intelligence Taskforce, and other international partners, coordinated to target a transnational narcotics trafficking syndicate and network that laundered not just the narcotics trafficking syndicate's funds, but also those of cartels, biker gangs, terrorist organizations, organized crime groups, and sanctioned entities.

The operation used: (1) BSA data, including the lead information generated from reports; (2) public-private partnership data such as information from financial institutions engaged in cooperation under section 314(b) of the USA PATRIOT Act; (3) data obtained from the public-private information-sharing program FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act; and (4) data from additional investigative efforts. The investigation resulted in the indictment of several subjects in and outside of the United States and the subsequent sanctions designation of a financial exchange by Treasury's Office of Foreign Assets Control. The investigation involved more than $1 million in sting transactions, international wiretaps, pen registers, and significant human intelligence and undercover work.

The target narcotics syndicate grossed annual revenue estimated in the multi-billion dollar range, and the money laundering organization laundered more than $270 million for the narcotics traffickers during an 18-month period. The target exchange conducted approximately 29,000 wires for approximately $687,000,000 over six years. Forensic accountants used complex analytics to review the BSA data and other financial records to identify the criminal transactions in U.S. bank wire entries and trace illicit proceeds across three continents.

U.S. law enforcement agencies and foreign partners seized approximately $30 million of illicit proceeds; 5,300 kilograms of cocaine; 1,300 kilograms of methamphetamine; 90 kilograms of heroin; 369 gallons of methamphetamine precursor chemicals; a narcotics laboratory; a yacht; and semi-automatic weapons. The operation resulted in 30 OFAC sanctions designations, international arrests, 24 domestic indictments, and an additional forfeiture judgment of approximately $6,350,000.

The U.S. Attorney's Offices of the Southern District of New York and the Southern District of Florida prosecuted the cases, with assistance from the Southern District of Texas.

Cybercrime – *U.S. Secret Service and U.S. Postal Inspection Service*

The U.S. Secret Service and the U.S. Postal Inspection Service began investigating a business email compromise (BEC) ring operating in a U.S. metropolitan area. This investigation focused on the individuals laundering the proceeds from the BEC scheme. BEC schemes exploit the fact that many rely on email to conduct business. In a BEC scheme, conspirators infiltrate the computer systems of victim companies, including their email servers and email accounts, through phishing attacks or the use of malware and use this access to pose as company employees and steal funds from the victim company. The conspirators in this scheme impersonated victims' business partners when a payment was due and claimed the business partner's bank account information had changed. Then, intending to send the money to the business partner, the victim businesses instead sent the money to bank accounts controlled by the conspirators. According to the Internet Crime Complaint Center (IC3), BEC schemes generate the highest losses—$2.4 billion in 2021—among all categories of internet crime, including ransomware.

In this case, the co-conspirators' bank accounts were associated with payments representing victim losses of more than $6.7 million. U.S. law enforcement arrested four subjects on Federal charges. One subject immediately pled to conspiracy to commit money laundering and was sentenced to 15 months. Shortly after, another subject pled to conspiracy to commit money laundering and was sentenced to 15 months. The final two subjects elected to go to trial, where a Federal jury convicted

one of the subjects of several counts of substantive money laundering and the other subject of several counts of structuring. Both subjects were convicted of conspiracy to commit money laundering. The subjects were sentenced to 120 months and 51 months, respectively.

The nature of the BEC scheme made BSA data instrumental and essential in the case, from the initial lead discovery and development to the final stages of the investigation and prosecution. The BSA information obtained in this investigation was crucial to identifying accounts and identifying the co-conspirators, ultimately leading to the successful conviction of the co-conspirators.

The U.S. Attorney's Office, Eastern District of Virginia prosecuted this case.

Proliferation Financing – *The Department of Defense Office of Inspector General, Defense Criminal Investigative Service, and the Department of Homeland Security - Homeland Security Investigations*

The Defense Criminal Investigative Service and Homeland Security Investigations initiated an investigation into a fraud and proliferation financing scheme involving the fraudulent representation of a contracting official.

Targets of the investigation established and used what was purported to be a U.S. Navy email address; authentic forms, titles, addresses; and other indicia to pose as a U.S. government contracting agent to fraudulently obtain merchandise, including various electronics and specialized communications equipment. The specialized communications equipment was controlled for export under the International Trafficking in Arms Regulations (ITAR) and valued at approximately $3.2 million. The electronics were valued at approximately $8 million.

Three victim companies—one that provided wireless voice and data services; one that was a wholesale audio-video distributor and manufacturer's representative; and one defense contractor that designed, manufactured, and marketed communications equipment—shipped the merchandise, without prior payment, to co-conspirators on the East Coast. Those individuals then shipped the stolen items to other co-conspirators on the West Coast, where they were sold.

From the onset of the investigation, the primary goal of the investigative team was to recover the stolen ITAR-controlled specialized communications equipment. After investigators had exhausted traditional means to track and trace the equipment and affirmatively uncover evidence of export violations, agents pivoted to focus the investigation on the laundering of the proceeds of the stolen goods. Agents who had attended FinCEN training sessions recognized the need to use the public-private information sharing program that FinCEN operates under section 314(a) of the USA PATRIOT Act as well as the cross-border information sharing channel FinCEN provides through the Egmont Group of FIUs. Responses to their requests provided essential information to aid in the investigation. Specifically, the 314(a) responses provided information to support the issuance of more than 20 subpoenas to various financial institutions, many of which were local credit unions that were previously unknown to the investigators. These subpoenas proved indispensable to the ultimate outcome of the investigation.

Using source information and shipping documents, agents traced the stolen goods to the West Coast. Using information obtained from the 314(a) program and BSA reporting, agents were able to identify cash deposits, commonly structured to evade currency transaction reporting thresholds.

Specifically, to avoid triggering currency reporting requirements, a large portion of the transactions used to promote the ongoing criminal conspiracy were made in the form of "Out of State" cash deposits at ATMs and to bank tellers.

To underline the importance of the FinCEN programs used in this investigation, the information included in BSA filings as well as responses to investigators' 314(a) requests led to nine defendants being charged with, among other things, conspiracy to commit money laundering and conspiracy to commit mail and wire fraud. To date, defendants have been ordered to serve a total of more than 22 years' incarceration. Law enforcement recovered approximately $3 million worth of electronics and communications equipment and the courts ordered the defendants to pay $4,494,882 in restitution. Forfeiture orders of approximately $520,994 were also filed.

This case was prosecuted by the U.S. Attorney's Office, District of Maryland.

NOMINATED CASES

Cybercrime – *Federal Bureau of Investigation*

Information from dozens of BSA reports assisted the Federal Bureau of Investigation (FBI) in unravelling a complex financial crime and cyber banking scheme in which victims lost more than $50 million to fake investments and a multinational financial institution had its identity stolen.

The scheme to defraud investors allegedly started in late 2012, when an individual devised a plan to obtain money from prospective investors by posing as an executive and owner of a bank on the West Coast who was about to purchase a small legitimate state-chartered bank. The subject falsified official documents to support the claim. The subject also counterfeited documents that would indicate to an investor an established banking relationship with a multinational bank. In essence, the subject stole the identity of the legitimate bank.

From 2012 to 2020, the main subjects and others engaged in an internet-based financial fraud scheme, which generally involved the creation of fraudulent websites to solicit funds from investors. Victims of the fraud scheme typically discovered the websites via internet searches. These websites advertised various types of investment opportunities, most prominently the purchase of certificates of deposit (CD) advertised at higher-than-average rates of return, to lure potential victims.

The subject provided the victims with applications and wiring instructions for the purchase of a CD. The funds wired by the victims were then moved to various domestic and international bank accounts. The subject targeted very sophisticated investors and CD brokers, and victims included a municipal government and a large credit union.

However, soon after investors wired over half a million dollars to the subject's account, one of the investors became suspicious and notified the FBI. Other investors, including the multinational bank, also became suspicious and began conducting investigations. Because of the numerous inquiries, the multinational bank became aware of the false documents and filed BSA reports on the subject.

FinCEN's 3l 4(b) Program enabled participating financial institutions to work together and share information, resulting in the closing of suspect accounts and slowing the spread of the fraud. Financial institutions also used the 314(b) program to identify dozens of previously unknown accounts used to facilitate the funneling of approximately $50 million in illicit fraud proceeds to multiple individuals through the international money laundering ring.

To date, at least 150 fraudulent websites created as part of the scheme have been identified. At least 70 victims of the fraud scheme nationwide, many of whom were elderly, collectively transmitted approximately $50 million that they believed to be investments.

The subjects were arrested and admitted to conspiring to commit wire and securities fraud in connection with their roles in a $50 million cyber internet fraud scheme. The main subject was released on bond pending sentencing, and the other subject is serving a 45-month sentence. The U.S. Attorney's Office for the District of New Jersey prosecuted the case.

Fraud – *Federal Bureau of Investigation*

Based on an allegation received from a Medicare contractor, the Federal Bureau of Investigation along with the U.S. Department of Health and Human Services, Office of Inspector General opened multiple joint investigations into suspect home health agencies (HHAs) that had a questionable spike in claims.

Investigators initially believed the fraud was being perpetrated by separate and distinct entities and opened three separate investigations. However, after reviewing BSA reporting, the financial connections between the entities became clear. In particular, one report revealed the nature and extent of the network underlying aspects of the fraud scheme and provided significant leads to investigators. BSA reporting accelerated the financial investigation and likely saved investigators as much as six months in building their case.

The primary subject orchestrated a scheme to defraud Medicare of approximately $48 million by billing for nursing and physical therapy services that were never provided. Over the course of the scheme, the subject acquired 26 HHAs that were collectively controlled through one company he owned. The primary subject enlisted multiple co-conspirators to acquire the HHAs using aliases and false identification to effectively disguise the HHAs' true ownership.

Most of the proceeds of the fraud were laundered through a hawala scheme in which individuals living in other countries contacted brokers who arranged money transfers to individuals in the United States using the funds stolen from the Medicare program. Approximately 1,500 entities and individuals were paid by the suspect's company through this scheme.

To date, ten subjects have been charged and six have pleaded guilty. The four remaining indicted subjects are fugitives. More than $3.5 million was seized as a result of the investigation and financial analysis. The first subject was sentenced to 12 years imprisonment and more than $48 million in restitution.

The U.S. Attorney's Office for the Northern District of Illinois prosecuted this case.

Fraud – *United States Marshals Service*

The U.S. Marshals Service, the U.S. Department of Health and Human Services Office of Inspector General, and the Federal Bureau of Investigation investigated a potential Medicare fraud scheme.

The investigation revealed a company providing medical services, under the direction and control of two individuals, engaged in a scheme along with another company to defraud Medicare through the submission of false claims for durable medical equipment services.

Through BSA reporting, investigators identified financial accounts utilized in the fraud, traced the movement of the fraud proceeds, and identified potential assets obtained with the proceeds that could be subject to forfeiture.

Investigators also used the public-private information-sharing program FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act to identify a previously unknown account. FinCEN also reached out via Egmont Group channels to a country that was identified in the wire transfer activity to request additional information.

The activity resulted in the submission of approximately $4,172,553 in fraudulent claims filed to Medicare for reimbursement.

BSA reporting depicted deposits into the suspect financial accounts. Assets valued at more than $3.6 million were identified through the accounts to include a $2,344,018.82 in real estate property, $1,097,279.22 in U.S. currency, and $164,827.80 in luxury jewelry, which accounted for approximately 86 percent of the total amount defrauded.

The U.S. Attorney's Office for the Middle District of Tennessee prosecuted the case.

Cybercrime – *Internal Revenue Service-Criminal Investigation and Federal Bureau of Investigation*

The Internal Revenue Service-Criminal Investigation and the Federal Bureau of Investigation began investigating a stolen identity tax refund fraud case for a refund of $937,914. BSA filings allowed agents to track refund withdrawals in cash structured at different locations in Florida, Georgia, and Alabama. Three subjects were identified, in part due to these filings. The investigation revealed 48 additional false tax returns in the subjects' names and the names of identity theft victims. In total, these additional false returns claimed more than $40 million in tax refunds; $12.3 million in actual fraudulent refunds were issued.

To obtain these massive refunds, the conspirators used a little known but highly abused tax credit scheme, called the "off-highway business use" fuel tax credit. "Off-highway business use" refers to fuel used in a trade or business or in an income-producing activity for vehicles and equipment such as generators, compressors, power saws, and in forklifts, bulldozers, and earthmovers. The subjects claimed to have utilized 52,654,920 gallons of "off-road" gasoline.

The subjects also laundered their ill-gotten gains through several accounts and used significant portions of the fraudulent tax refunds to purchase real estate and other assets.

Financial institutions where the subjects laundered their funds filed several BSA reports that were instrumental in allowing the agents to locate, freeze, and ultimately seize and forfeit the funds. The agents recovered approximately $6 million from eighteen accounts located at nine different financial institutions, two vehicles, and three houses.

The primary subject pled guilty to conspiracy to commit wire fraud, conspiracy to commit money laundering, and aggravated identity theft, and was sentenced to 19 years and 6 months in Federal prison with a $12.3 million forfeiture order.

The U.S. Attorney's Office for the Middle District of Florida prosecuted the case.

Fraud – *Federal Deposit Insurance Corporation-Office of Inspector General*

Based on information contained in BSA reporting, the Federal Deposit Insurance Corporation-Office of Inspector General and the Federal Bureau of Investigation began to look into the activities of an individual who was running a sophisticated fraud scheme targeting government programs created or supplemented by the CARES Act.

Information in the BSA reporting revealed 17 related business entities and 30 different bank accounts associated with the subject and their co-conspirator. They were utilizing numerous shell companies and apparently dormant business entities as part of this scheme.

Investigators conducted an exhaustive review of the accounts that showed a clearer picture of how the subject was attempting to obfuscate the funds they received from the loans as well as the fact that a large portion of the money was spent on expenses that were not authorized under the CARES Act. The volume, duration, and scope of the subject's criminal conduct was staggering.

The subject pled guilty to conspiracy to commit wire fraud and bank fraud and was sentenced to serve 41 months in prison to be followed by 60 months of supervised release for their role in fraudulently obtaining funds from the Paycheck Protection Program. The subject was held accountable for a fraud loss of over $1.7 million. As part of the sentence, the subject was ordered to pay restitution of almost $1.2 million to the victims.

This case was prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia.

Drug Trafficking Organization Activity – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation, as part of the Financial Investigations and Border Crimes Task Force, initiated an investigation into a tax preparation business after discovering a number of BSA reports related to the business. An analysis of the filings found that the co- owners were opening bank accounts for various business entities with multiple financial institutions (small, medium, and large sized) throughout the area.

Further analysis determined that the company created several shell corporations to open bank accounts for co-conspirators for the sole purpose of facilitating the placement and layering of more than $42 million of drug trafficking proceeds into the U.S. financial system.

The transactions included thousands of structured cash deposits made via ATMs in several major cities across the United States. After several layering transactions, the funds were wired to one of several bank accounts located in Latin America. By working with FinCEN to reach out to foreign counterparts via Egmont Group channels, investigators were able to confirm the owners of the accounts.

The efforts of investigators resulted in the prosecution of four individuals who laundered more than $42 million in drug trafficking proceeds on behalf of a Sinaloa-based drug trafficking organization.

The U.S. Attorney's Office for the Southern District of California prosecuted the case.

Fraud – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation initiated this investigation as a direct result of BSA reporting that provided various key pieces of information into an international criminal organization that laundered funds from various fraud schemes, including romance fraud and CARES Act fraud. As the investigation continued, additional BSA reporting allowed investigators to identify numerous accounts, several co-conspirators, and victims.

The investigation revealed scammers who were creating fictitious profiles on online dating websites and social media platforms. The scammers cultivated romantic relationships with victims, eventually asking them for money. The fraudsters worked in concert with co-conspirators who accepted the victims' money and transmitted it, through various means, to the scammers. Means of transmission of funds included the purchase and of salvaged automobiles and a complex system of trade-based money laundering.

The primary subject and six other co-conspirators were convicted and sentenced to a total of 186 months for laundering the proceeds of online romance scams. The total amount generated by romance fraud that these individuals laundered was more than $11.8 million. Two hundred and thirteen victims from 43 states and 13 countries spanning five continents were affected by this fraudulent scheme.

The U.S. Attorney's Office for the Southern District of Ohio prosecuted the case.

Fraud – *Air Force Office of Special Investigations*

The Air Force Office of Special Investigations initiated an investigation based upon a BSA report indicating what the reporting institution judged to be an individual's attempt to negotiate and electronically wire proceeds derived from the deposit of a counterfeit obligation totaling $79,000 to an unidentified recipient located overseas.

Additional law enforcement record checks disclosed that the subject, along with other conspirators, defrauded a financial institution by negotiating counterfeit obligations endorsed to other individuals via remote online deposits. The primary subject engaged in similar patterns of behavior with several other financial institutions.

Financial records confirmed the subject completed more than $49,000 in electronic funds transfers to various subjects located overseas. Financial analysis further revealed that during a nearly four-year period, the subject conducted almost 1,700 financial transactions totaling more than $500,000.

The subject was charged with felony forgery and sentenced to up to 36 months imprisonment. The investigation was successfully prosecuted by the U.S. Attorney's Office for the District of Nevada.

Fraud – *United States Secret Service*

The United States Secret Service initiated an investigation involving an illegal firearm and a stolen rental car that was located at the scene. Initial investigative efforts began with BSA data analysis. This analysis led to the discovery of a fraudulent scheme involving loans and benefits made available by the CARES Act.

The investigation revealed that a subject was receiving multiple suspicious CARES Act unemployment payments as well as a Small Business Administration Paycheck Protection Program loan. Further review of additional BSA reporting indicated the subject had several other claims and loans filed in their name as well as other individuals' personally identifiable information. The analysis revealed numerous email accounts which were used in association with the claims and loans that were linked directly to the subject's residence.

The suspect plead guilty to wire fraud, false representation of a Social Security Number, aggravated identity theft, felon in possession of firearm and ammunition, and possession with intent to distribute 40 grams or more of fentanyl and was sentenced to 94 months in prison and four years of supervised release.

The U.S. Attorney's Office for the District of Massachusetts prosecuted this case.

Fraud – *Diplomatic Security Service*

The Diplomatic Security Service Chicago Field Office began investigating a passport renewal for fraud after a systems check showed the passport recipient as deceased. Facial recognition and additional research proved the applicant held a valid passport under their own name.

During the initial investigation, it was determined that the defendant had assumed the identity of a deceased child and first began using the assumed identity in 2003. Under the assumed identity, the defendant received a Social Security Number, held a Student Pilots License, was employed as a flight attendant, and had multiple businesses registered in Ohio.

Investigators searched BSA records for both the defendant's assumed and actual identities, which revealed that the defendant had applied for 20 Small Business Administration Paycheck Protection Program loans under the assumed identity, and was approved for 16, collectively worth approximately $1.6 million. A financial institution had denied a bank loan due to fraud concerns after determining that the subject had submitted forged documents in conjunction with the application. Additional reports showed apparent structuring of funds, potential mortgage fraud, and wire transfers between the actual defendant and their alias. Ultimately, BSA data revealed many potential financial crimes that were previously unknown to investigators, as well as 30 financial accounts for both the defendant and the assumed identity. BSA records also assisted in revealing the destination of funds, including the purchase of luxury real estate.

The defendant has pled guilty to fifteen counts of wire fraud and one count of passport fraud and remains in custody until a sentencing hearing. The plea included a forfeiture judgement of $1.5 million and the forfeiture of two pieces of luxury residential real estate.

The U.S. Attorney's Office for the Southern District of Ohio prosecuted this case.

Corruption – *Federal Bureau of Investigation and U.S. Department of Agriculture-Office of Inspector General*

The FBI reviewed BSA data that revealed reports filed on a personal checking account and business account for a not-for-profit organization with more than $10.7 million worth of suspicious deposits and payments. There were deposits from the State of Illinois via Automated Clearing

House credits, which were followed by cash withdrawals from ATM locations and large checks issued to a third party. The not-for-profit ran a religious institution, childcare center, nutrition services, and a private school. An associated report listed a sub-grant from the U.S. Department of Agriculture (USDA) under the Child and Adult Care Food Program and the Summer Food Service Program. The not-for-profit received more than $8.4 million in grant funds intended to serve at-risk youth that was instead embezzled by the defendant. USDA Office of Inspector General was engaged as an investigative partner.

BSA data assisted in linking additional financial accounts along with persons and entities of interest associated with the suspicious financial activity. Investigation showed the not-for-profit had overbilled more than $1 million in a two-month period and the defendant used fraudulently acquired USDA funds to pay for personal travel, elective medical expenses, and luxury automobiles.

Further investigation revealed a parallel fraud scheme involving separate Federal program funds administered by area public schools to offer a "Safe Haven" for students during critical high violence periods. Law enforcement was alerted to the involvement of a former public school executive who oversaw the Safe Haven Program. Through interviews and the review of emails and program records, investigators identified a kickback scheme with a nexus to a corrupt public official. The executive and defendant conspired to inflate the number of sites and children for the federally funded Safe Haven Program so the defendant could fraudulently obtain additional funds for meals that were not provided. In exchange, the executive received approximately $150,000 in kickbacks.

The defendant pled guilty to one count of mail fraud, was sentenced to 51 months imprisonment, followed by a one-year period of supervised release, and ordered to pay restitution of $1,054,689 to the USDA. The former public school executive died prior to being indicted.

The U.S. Attorney's Office for the Northern District of Illinois prosecuted this case.

Drug Trafficking Organization Activity – *Drug Enforcement Administration*

The Drug Enforcement Administration initiated a multi-agency investigation into an illegal marijuana distribution conspiracy. The catalyst of the investigation was several BSA reports related to the primary suspect and their straw business. The primary suspect, along with several co-conspirators, illegally distributed marijuana valued more than $3 million annually, using the straw business to launder the proceeds.

Search, seizure, and arrest warrants were executed on several locations associated with the money laundering and marijuana distribution investigation. More than 150 kilograms of marijuana and related contraband were seized, along with evidence associated with distribution and money laundering.

The primary subject was charged with conspiracy to distribute controlled substances, conspiracy to commit money laundering, and money laundering, and faces up to 20 years in prison.

The U.S. Attorney's Office for the Eastern District of Virginia prosecuted this case.

Fraud – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation (IRS-CI) was provided information on a check casher who was allegedly cashing checks in amounts over $10,000 but would not file the proper paperwork. An initial review of BSA data showed the check casher was a registered money services business, but it also showed a pattern of activity that prompted IRS-CI to initiate an investigation.

Investigators used the available BSA reporting by the checker casher to find customers who were potentially using the business to avoid filing BSA reports. From prior experience, investigators were aware of schemes where companies used check cashers to avoid paying payroll and income taxes.

While canvasing the BSA data for potential cooperating defendants, a search warrant was executed on the business. The search warrant seized customer files, Currency Transaction Reports, and other financial business records. At the time of the search warrant, individuals were interviewed and verified that the business failed to file the proper paperwork at the direction of the owner.

Investigators also utilized FinCEN's BSA Record Certification Program, requesting certification of more than 21,000 BSA reports. The documents provided were invaluable.

Ultimately, the owner pled guilty to structuring financial transactions and payroll tax evasion and was sentenced to 48 months imprisonment with 2 years of supervised release. Additionally, the owner was ordered to pay more than $590,000 in restitution to the IRS and more than $250,000 in forfeiture.

The U.S. Attorney's Office for the Eastern District of New York prosecuted the case.

Fraud – *Department of Defense, Defense Criminal Investigative Service*

The Defense Criminal Investigative Service (DCIS) initiated an investigation into potential procurement fraud being conducted by a military civilian employee overseeing a foreign U.S. Army base's public works program. More than $3 billion was awarded to a contractor to assist in support operations at the U.S. Army base.

The defendant civilian employee oversaw projects under this contract from approximately 2007 to 2016. The defendant was involved in the solicitation, award, and management of government contracts to include heating, ventilation, and air-conditioning projects at the base. The defendant held various roles throughout the procurement process, including project manager, mechanical engineer, project engineer, and contracting officer representative.

A local subcontractor bid on several of the projects under the contract. The subcontractor's general manager and company co-owner was a known acquaintance of the defendant, with documented communications about projects, or potential projects, on U.S. military installations, to include subcontracts under this contract.

Together with other co-conspirators, the defendant and subcontractor steered contracts to the subcontractor and artificially inflated costs between 14 and 25percent, with the co-conspirators splitting the illicit proceeds. To help obfuscate the illicit arrangement, funds were wired to an immediate family member of the defendant.

BSA data was vital in identifying potential bank accounts and account owners involved in the fraud scheme, as well as additional probative information. DCIS used information obtained via the public-private information sharing program that FinCEN administers pursuant to section 314(a) of the USA PATRIOT Act, in combination with previously obtained BSA data, which allowed for an in-depth link analysis of the defendant family's financial accounts. DCIS also worked with FinCEN to reach out to international partners via Egmont Group channels to obtain records from the countries of origin and destination for the relevant international transactions.

The defendant pled guilty to conspiracy, kickbacks, and aiding and abetting, and was sentenced to two years imprisonment. The subcontractor pled guilty to illegal gratuities and was sentenced to two years imprisonment, to be served in his home country.

The U.S. Department of Justice, Criminal Division, Fraud Section prosecuted the case.

Fraud – *United States Secret Service*

In September 2018, the U.S. Attorney's Office for the Middle District of Florida received notification from a credit card company regarding several suspicious purchases made on government credit cards issued to a tax collector's office in the state of Florida. The United States Secret Service (USSS) Orlando Field Office investigated the case.

The USSS utilized FinCEN resources to assist with this investigation, participated in FinCEN training sessions, and accessed educational material—more specifically, content relating to virtual currencies.

Upon review of all the evidence recovered in this investigation, to include numerous witness and suspect interviews, a clear pattern of corruption involving kickbacks, bribery, wire fraud, aggravated identity theft, production of false identification, stalking, and sex trafficking of a child was uncovered.

A Federal grand jury indicted an official within the tax collector's office in June 2020 on numerous Federal charges, including stalking and identity theft. In late June 2020, the defendant resigned from his position. Additional evidence resulted in two superseding grand jury indictments. The defendant was subsequently indicted on identity theft, aggravated identity theft, sex trafficking of a minor, and the unauthorized use of personal identifying information.

In late February 2021, the defendant was arrested because he violated his terms of Federal probation, which included purchasing a firearm and traveling to another state. The subject was indicted once again and charged with 33 additional counts, including wire fraud, aggravated identity theft, conspiracy to bribe a public official, submission of a false claim, theft of government property, three counts of illegal monetary transactions, and numerous counts of production of false identification documents.

This investigation leveraged multiple partnerships, including with the Federal Bureau of Investigation, U.S. Small Business Administration Office of Inspector General, Seminole County Sheriff's Office, and the Florida Highway Patrol. This joint investigation, which required coordinating resources and personnel, further resulted in forfeiture of sports memorabilia and a $1.9 million restitution agreement.

In May 2021, the defendant pled guilty to six Federal charges: sex trafficking of a child, production of a false identification document, aggravated identity theft, wire fraud, stalking, and conspiracy. The defendant was sentenced to 11 years imprisonment.

The U.S. Attorney's Office for the Middle District of Florida prosecuted this case.

Fraud – *Internal Revenue Service- Criminal Investigation*

The Internal Revenue Service-Criminal Investigation (IRS-CI) investigated a group of co-conspirators who were filing frivolous tax returns for sham trusts. The co-conspirators attempted to receive more than $2.9 billion in erroneous tax refunds. Despite the best efforts of the IRS, the co-conspirators received more than $5.6 million in erroneous tax refunds. The tax refunds were deposited into bank accounts controlled by the co-conspirators and used for their personal benefit, including the purchase of a personal residence and multiple luxury vehicles.

To locate the scheme's organizer prior to indictment, IRS-CI checked records maintained by FinCEN and discovered that BSA reports had been filed on the defendant for attempting to negotiate U.S. Treasury checks issued to sham trusts he controlled, facts that were previously unknown to IRS-CI. The BSA data led to additional information, such as frivolous tax returns filed by the co-conspirators. The tax returns which were filed that generated the erroneous tax refunds described in the BSA data were used for mail fraud counts in the indictment against the conspirators.

The scheme's organizer pled guilty and was sentenced to 14 years imprisonment. A second co-conspirator was found guilty at trial and is scheduled for sentencing.

The U.S. Attorney's Office for the Middle District of Florida prosecuted this case.

Fraud – *Bureau of Alcohol, Tobacco, and Firearms*

Based on a single BSA report, the Bureau of Alcohol, Tobacco, and Firearms initiated an investigation into an individual suspected of a fraud scheme involving firearms and other goods.

After obtaining additional information, investigators were able to identify and analyze numerous accounts associated with the subject as well as victims of the fraudulent activity. Further analysis of BSA reporting revealed that the subject was using numerous aliases, email addresses, and financial accounts in false and fraudulent names. Using these fictitious and fraudulent accounts, the subject would order high-value products from individual sellers and retailers online and successfully divert the packages mid-shipment, sometimes by posing as the seller or shipper. After taking possession of the packages, the subject filed claims that the items were not received, causing the purchase price to be refunded and allowing the subject to obtain both the product and the money. Using this method, the subject defrauded at least 27 victims in 17 states.

The subject was sentenced to five years in Federal prison after pleading guilty to wire fraud and possession of stolen firearms.

The U.S. Attorney's Office for the District of South Carolina prosecuted this case.

Fraud – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation initiated an investigation involving the breach of two separate certified public accountant firms' computer servers. The personal identifiable information (PII) data acquired from the breach was used to file fraudulent Federal income tax returns totaling more than $20 million in tax refunds, of which more than $6 million was issued.

The U.S. Treasury checks were mailed to victims' home addresses. However, the co-conspirators redirected mail by filing fraudulent mail forwarding requests online through the U.S. Postal Service website, directing the mail to be delivered to controlled addresses.

Using the bank account information listed on the fraudulent returns, investigators searched BSA reporting and discovered that financial institutions had filed numerous BSA reports because the accounts had received multiple tax refunds, and the funds were quickly moved. While the financial information listed different addresses, investigators were able to determine the account holder for one of the accounts resided at one of the addresses that received a Treasury check that was re-routed.

Investigators were able to recover Treasury checks that individuals attempted to deposit into bank accounts. By searching BSA records for the victims' PII, investigators were able to identify bank accounts that had been established with the stolen PII.

The availability of BSA reporting was instrumental in identifying near-real-time information that investigators acted on during the investigation. Ultimately, allowed investigators to recover millions of dollars in fraudulent tax refunds and identify dozens of other firms whose data had been breached, as well as identify the thousands of victims whose PII was being used in these frauds.

In total, investigators were able to identify 50 additional breaches of firms and computer servers across the United States. These breaches were traced to more than $100 million in fraudulent claims made against the U.S. Government. The final indictment included $60 million of these false claims.

The subject and their co-conspirators were sentenced to a total of 90 months in Federal prison.

The U.S. Attorney's Office for the Middle District of Florida prosecuted this case.

Fraud – *New York State Department of Taxation and Finance*

The New York State Department of Taxation and Finance's Office of Internal Affairs initiated an investigation into a fraud ring that operated in a large metropolitan area.

BSA reports helped identify the primary subject's aliases and identify other subjects, which resulted in expanding the case to two U.S. Attorneys' Offices. BSA reporting showed a bank account where stolen checks were deposited, which led to the discovery of several other accounts into which fraudulent checks had been deposited.

The primary subject was arrested and charged with a scheme that caused $1 million in losses and was sentenced to 27 months in Federal prison. Several co-conspirators were arrested, found guilty, and sentenced to a total of 181 months in Federal prison. Their participation in this scheme resulted in more than $3.7 million in losses.

More than $4 million in restitution was ordered to be paid by the defendants.

The U.S. Attorney's Office for the Southern District of New York and the U.S. Attorney's Office for the District of New Jersey prosecuted this case.

Fraud – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation initiated this investigation based on a victim complaint indicating that the perpetrator—someone the victim met on an internet dating site—claimed to have been in a car accident in which the other driver suffered deadly injuries. The perpetrator further claimed to be in the hospital and under arrest for manslaughter, and then introduced an attorney requesting funds from the victim. The victim was directed to deposit cashier's checks into a business account and then wire the funds to a business account at another financial institution. Both bank accounts were in the name of the same business.

The investigative team analyzed BSA data using the known bank account information and discovered multiple instances of alleged fraud reported by several financial institutions. One BSA report described activity suggestive of a business email compromise scheme in which the victim account holder was instructed to deposit $100,000 into the perpetrator-controlled business account, while another report described activity suggestive of a romance scam in which the victim loaned money to someone they met online who was living in Nigeria. In this second scheme, the perpetrator returned the loan with at least an extra $28,000 through a check purportedly drawn on a church. The victim wired the $28,000 to the business's bank account, only for the check drawn on the church to be returned as "account closed."

FinCEN's networking feature for agencies that search BSA data revealed several other agencies were involved in related investigations and aided with deconfliction efforts. Other agencies with investigations identified the perpetrator as a bitcoin broker or exchanger. While these developments added a layer of complexity and coordination to ensure the integrity of all investigations, they allowed for increased collaboration and the prevention of duplicative efforts.

In addition to controlling accounts associated with romance, business email compromise, narcotics, and elder fraud schemes, the subject was identified as a bitcoin exchanger. Open source and bank records indicated the subject owned and operated bitcoin ATMs in and around the Austin, TX area, advertising cryptocurrency exchange services on Craigslist.org and Localbitcoins.com, claiming they had the ability to conduct $100,000 transactions anonymously.

The subject was indicted on seven counts in violation of money laundering and structuring financial transactions and later entered a guilty plea to one count in violation of operating an unlicensed money transmitting business. In the guilty plea, the subject admitted to moving more than $3,000,000 through their personal and business bank accounts. The subject was sentenced to 41 months in prison, with credit for time served, and 36 months of supervised release. The seizures of $93,865 were ordered forfeited and the subject was also ordered to pay $562,452.24 in victim restitution, to be prorated amongst eight victims.

The U.S. Attorney's Office for the District of Arizona prosecuted the case.

Fraud – *Internal Revenue Service-Criminal Investigation & Federal Bureau of Investigation*

Valuable BSA reporting led the Internal Revenue Service-Criminal Investigation and the Federal Bureau of Investigation to initiate a case, develop leads, follow the money, and identify key players and associates during this financial fraud investigation involving securities and investments.

BSA reporting included crucial information to identify potential co- conspirators. Information contained in the BSA data assisted the investigators with identifying critical witnesses who were interviewed and identified financial accounts where additional evidence was obtained to support the investigation and ultimate prosecution of the defendants.

The primary subject acted as an investment adviser to his client, a city municipality. The subject promised an investment strategy with guaranteed returns. Instead, the subject purchased $9 million of U.S. Treasury notes with the city's funds and took out margin loans using the notes as collateral. In the months that followed, the subject and his co-conspirators misappropriated approximately $7.2 million that belonged to the city by transferring various sums to themselves, and entities they controlled, using brokerage accounts.

To carry out the scheme, the subject and his associates made material misrepresentations to City officials and falsified brokerage account documents and correspondence. To conceal the fraud, the subject advanced $1.8 million to the city, which represented the 10% annual interest the subject promised for two years. The $1.8 million was taken out from the $9 million initial investment the city made.

The subjects used these monies for personal expenses and purchases of personal and real estate property. Ultimately, five subjects pled guilty and two were convicted at trial.

The U.S. Attorney's Office for Puerto Rico prosecuted the case.

Fraud – *Internal Revenue Service-Criminal Investigation*

Internal Revenue Service-Criminal Investigation initiated an investigation into an online romance scheme involving the use of fictitious identities, the creation of dating profiles on various online dating websites, and the creation of numerous email accounts and voice over internet protocol phone numbers, to communicate with victims.

BSA data is extremely helpful in online romance scheme investigations, especially when it comes to identifying co-conspirators. The supporting documentation for the BSA reports regarding the victims' accounts reduce the need for additional investigative steps when only a small snapshot of activity is needed and provide valuable context when conducting victim interviews. In this investigation, BSA data revealed at least two nominees that were facilitating transactions on the primary subject's behalf and captured a few victim statements regarding reasons for the financial transactions.

The subject and his co-conspirators claimed to be members of the United States military who received, found, or were awarded gold bars and needed assistance in paying the fees and shipping costs associated with getting the gold bars to the United States. The victims were told they would be reimbursed once the gold bars arrived in the United States.

As instructed, victims wired money to bank accounts controlled by the primary subject and others. Investigators identified more than 80 victims of the romance scheme. In total, identified victims were defrauded out of more than $1.76 million.

The primary subject was arrested, pled guilty, and was sentenced to a 168-month term of imprisonment followed by 36 months of supervised release. The subject was ordered to pay restitution of more than $3 million to 36 victims, more than $380,000 to the Internal Revenue Service, more than $4,000 to the New Jersey Department of Health and Human Services, and more than $6,900 to the U.S. Department of Agriculture.

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

Fraud – *Federal Bureau of Investigation*

Based on a single BSA report, the Federal Bureau of Investigation initiated an investigation into a public official of a Minnesota town. The single report allowed the agents to follow additional leads related to the subject. As part of a fraud scheme, the subject forged the signatures of town officials on business checks and solicited signatures from town officials by falsely representing that the checks would be used to pay the town's bills. Instead, the funds were transferred into the subject's personal account.

The subject was able to conceal the fraud by excluding the unauthorized payments from the town's annual report. The subject misappropriated more than $650,000 of town funds. In addition to embezzling the funds, the subject used the illicitly obtained funds to gamble.

The subject was charged with one count of wire fraud, pled guilty, and was sentenced to 27 months in prison and ordered to pay restitution of $652,674.66.

The U.S. Attorney's Office for the District of Minnesota prosecuted the case.

Fraud – *United States Attorney's Office, Eastern District of Missouri*

In 2018, an individual was found guilty of conspiracy to commit bank fraud that was related to their participation in a telemarking fraud scheme that targeted elderly victims. Through this scheme, the subject and 20 other co-defendants generated millions of dollars in fraudulent funds. The defendant was ordered to pay approximately $4.2 million in restitution to victims of the fraud.

In 2022, a U.S. probation officer assistant contacted the Asset Recovery Unit for the U.S. Attorney's Office in St. Louis to inform the office that the probation officer was suspicious of the defendant's reported employment and finances. The defendant appeared to have ample funds available, but still owed more than $3 million in restitution and was barely making payments.

The Asset Recovery Unit began an investigation into the subject's finances. Information found in BSA reporting proved to be invaluable and shed light on how the subject was concealing assets and conducting questionable business operations, including some cryptocurrency transactions.

Utilizing this information, investigators filed three separate garnishments and issued multiple subpoenas in efforts to pursue the various assets, including the cryptocurrency. After some negotiation, the defendant paid their restitution in full – which resulted in more than $3 million going to the victims.

The U.S. Attorney's Office for the Eastern District of Missouri prosecuted this case.

Fraud – *Internal Revenue Service-Criminal Investigation*

Internal Revenue Service-Criminal Investigation initiated a case into an individual who was suspected of embezzling money from their employer. Upon reviewing BSA reporting, it was determined the suspect had set up various merchant accounts and made a series of corporate credit card charges to those merchant accounts. The subject then transferred the funds from the merchant accounts into a checking account she controlled that was held in the name of a business.

Information obtained from financial institutions was critical to investigators, as it allowed them to create a comprehensive picture of the financial facts of the case and to secure search and seizure warrants for the subject's residence. Agents discovered hundreds of thousands of dollars of jewelry, watches, handbags, and other luxury goods, all of which were seized as evidence.

When confronted with the evidence, the subject admitted to the scheme and indicated a willingness to plead guilty before an indictment. The perpetrator was sentenced to 36 months confinement, 3 years Federal probation, $4,870,768.87 restitution to their employer, and $1,219,339.00 restitution to the Internal Revenue Service.

The U.S. Attorney's Office for the Northern District of California prosecuted this case.

Fraud – *Federal Bureau of Investigation*

This investigation was initiated by the Federal Bureau of Investigation (FBI) initiated an investigation into two individuals based on complaints from local police and bank officials. BSA reporting revealed information suggesting that the two individuals, along with dozens of co-conspirators, were involved in many fraudulent schemes and scams, including advance fees, investment scams, and work from home jobs. The most common and most lucrative schemes in which they appeared to be involved, however, were romance scams.

Romance schemes generally involve conduct in which persons develop online romantic relationships under false pretenses. The persons feigning romantic interest are commonly referred to as "Yahoo boys." They frequently work under larger scam operators, often targeting elderly woman who are frequently emotionally vulnerable, lonely, and often have access to savings and retirement accounts. After feigning romantic interest, the Yahoo boys, preying on the compassion of vulnerable individuals, fabricate an urgent need for money.

The defendants in this case were not the Yahoo boys, but the money mules who conspired with them to launder illicit proceeds. The case, thus, focused on money mules located in the United States. To undertake a financial investigation like this, the FBI needed to identify bank accounts, obtain relevant data by subpoena, and review it. The identification of the accounts in this case was

excessively complex. BSA reporting was the primary tool to overcome these complexities. The investigators canvassed BSA reporting weekly to learn of new accounts and fake passport names related to the subjects.

The investigators could have never imagined the case would evolve into a series of indictments, the conviction of more than 20 defendants, and the identification of dozens of other actors. Investigators identified more than 1,000 victims, although countless victims remain unidentified and total losses stemming from these defendants alone reached significantly more than $35 million. Investigators identified more than 550 bank accounts throughout this case, most of which were identified through a review of hundreds of BSA reports. Simply stated, FinCEN's BSA reporting was the key to success in this investigation.

The primary subject was sentenced to 63 months in prison and three years of supervised release and was ordered to pay $8.4 million in restitution to the victims.

The U.S. Attorney's Office for the District of Utah prosecuted this case.

Fraud – *United States Postal Inspection Service*

The U.S. Postal Inspection Service received an investigative lead via a single BSA filing on an individual who was suspected to be conducting an online romance scam. Specifically, the subject was alleged to be using several aliases on various online dating websites, pretending to be a highly educated physician who was single and seeking a relationship. The subject reportedly befriended the women with whom he "matched" on the dating sites.

The investigation determined that shortly after meeting the women, the subject earned their trust and convinced them he was wealthy and offered to pay their financial debts. The amount of these debts ranged from $5,000 to $100,000. Once the women accepted his offer, the subject convinced them to share their financial account information. He then sent funds to their accounts, which resulted in the women receiving an instant notification from their creditors that their accounts balances were paid; thus, giving the women confidence that their suitor was legitimate.

While the women were convinced that their debts were paid, but before the payments had been fully posted to their accounts, the subject further convinced some of the women to borrow money and send him back thousands of dollars to cover things for him.

Additionally, he convinced some of the women to purchase high-end jewelry and Rolex watches for him (as a loan). Thinking their debts were paid, the women felt obligated to send the requested funds or to purchase jewelry and Rolex watches for him because they believed he had eliminated their debt. The women withdrew their own available funds, or sometimes applied for additional loans, and then sent thousands of dollars into the bank accounts he instructed. Some of these funds were deposited into bank accounts in the subject's name; however, some accounts were in the names of the subject's wife and elderly mother.

Within days after sending money to the subject, the victims were notified by their creditors that the funds sent to pay their debts were deemed invalid, usually due to insufficient funds. The subject discontinued his communication with the women. In some cases, the criminal conduct created a significant financial loss to the victims, to include bankruptcy.

The investigation also revealed that in late 2016, the subject first executed this fraud scheme while he was incarcerated in prison for unrelated prior convictions involving similar types of fraudulent conduct.

As noted above, the single BSA filing initially brought the suspect's activity to the attention of investigators. That one filing identified several of the fraud victims, and the places where the subject spent the fraud proceeds, such as casinos. Additional BSA filings enabled investigators to learn where the subject was selling the Rolex watches he fraudulently obtained from his victims. The BSA data also facilitated the identification of the suspect as the person who defrauded many of the victims who only knew him by one of his many aliases.

In addition to enabling investigators in this case to identify additional victims and follow the movement of the fraud proceeds, BSA data helped the prosecution team merge multiple victims' criminal complaints to local law enforcement around the country into one comprehensive Federal case. Once investigators opened an investigation into the subject based on the initial BSA filing, additional BSA reports allowed all other known victims to be included under the purview of this Federal case.

After a nearly two-year investigation, the subject was indicted for multiple counts of wire fraud and mail fraud, aggravated identity theft, and money laundering. The subject entered a guilty plea to all 25 counts of the indictment and was sentenced to a total of 108 months in prison followed by three years of supervised release. He was also ordered to pay $1,161,325.82 in restitution to more than 40 women who he victimized.

The U.S. Attorney's Office for the Northern District of Florida prosecuted this case.

Fraud – *Federal Bureau of Investigation*

The Federal Bureau of Investigation initiated an investigation into two businesses for fraudulent Paycheck Protection Program (PPP) loan applications.

BSA data played a vital role by providing the initial lead for investigators in identifying the two subjects associated with the fraud. The two subjects shared their fraudulent processes with at least 16 other individuals who then obtained their own fraudulent PPP loans. One of the 16 individuals was an active Phoenix, Arizona police officer who obtained more than $1,200,000 in fraudulent PPP funds while on duty. In total, the network of 18 individuals obtained more than $13,000,000 in fraudulent PPP funds through 18 different businesses.

Authorities seized several properties across several states, tour vehicles, and approximately $2,300,000 from multiple bank accounts. The defendants were charged with conspiracy to commit bank fraud, bank fraud, false statements to the government, and money laundering.

The U.S. Attorney's Office for the District of Arizona prosecuted this case.

Fraud – *United States Secret Service*

In July 2022, the United States Secret Service Atlanta Field Office began investigating a multi-level embezzlement scheme involving a significant flow of funds between various bank accounts. The suspicious activity took place in the form of Automated Clearing House credits, debits, and large-

amount wire transfers between the accounts. Using BSA data, the Atlanta Field Office began analyzing the transactions, investigating subjects, and verified initial indicators of wholesale financial embezzlement.

This extensive investigation confirmed a multi-level embezzlement scheme with an unusually large and significant flow of funds involving a major retailer. The scheme involved two current employees of the retailer, one former employee, and external co-conspirators. Ultimately two defendants pled guilty to defrauding the retailer and embezzling $9.4 million while employed at the company in managerial and loss prevention roles.

One defendant worked as a manager at the company's warehouse. In their position, they supervised others and acted with authority to approve new vendors and the payment of vendor invoices. The other defendant was a loss prevention supervisor, who was also responsible for monitoring security risks, and protecting people, products, and information.

The manager provided fictitious vendor information to unknowing subordinates and asked them to input the information into the company vendor system. Once the information was entered, the manager approved the fictitious vendors, thereby enabling those vendor accounts to submit invoices. The manager recruited other individuals to act as purported vendor contacts for the fake vendors. They recruited the loss prevention supervisor into the scheme to supply information that could be used to fabricate vendor contacts. The co-conspirators submitted fabricated invoices for payment. These invoices falsely represented that the fictitious vendors provided goods and services. The payments for these invoices went to bank accounts controlled by the co-conspirators.

Ultimately, more than $10 million in fabricated invoices for fictitious vendors were submitted, with approximately $9.4 million paid to the co-conspirators. The proceeds were traced with the assistance of BSA data to real estate, luxury cars, and expensive jewelry.

The U.S. Attorney's Office for the Northern District of Georgia prosecuted this case.

Cybercrime – *Homeland Security Investigations*

Homeland Security Investigations (HSI) received a referral regarding the exploitation of the COVID-19 pandemic. The victim ordered hand sanitizer from a website and never received the product. Records provided by the victim showed that the payment was submitted through a U.S.-based payment processor. Although the two purchases were made only one day apart, the payment went to two different subjects' accounts. A search of the website by agents showed that it purported to sell numerous products that were name-brand health and safety items which were in high demand during the COVID-19 pandemic.

An administrative subpoena was issued to the U.S. based payment processor for records related to the two subjects. The records showed one subject received 1,336 payments totaling more than $27,000 between March 4, 2020, and March 27, 2020. The second account received more than 1,700 payments totaling more than $40,000 between March 3, 2020, and March 23, 2020. These accounts had numerous complaints alleging non-delivery of goods and investigators identified other websites that the suspects may have been using. Agents contacted the payment processor's COVID-19 response team and informed them of the fraud related to their investigation in an attempt to proactively disable suspected accounts and refund the victim's money, which the payment processor agreed to do.

With information provided by the case agents, the payment processor conducted their own investigation which resulted in them filing multiple BSA reports. The investigative team utilized these filings to identify additional accounts and websites that were connected to the organization. The supporting documentation showed that each account being used by the organization had a corresponding foreign identification card in the name of the account and led to the discovery that the organization was utilizing fraudulent UPS tracking numbers to have the payment processor side with the suspects in any dispute.

HSI Special Agents subpoenaed for information connected to known fraudulent websites that were identified by the supporting documentation along with information obtained from the Federal Trade Commission Consumer Sentinel Network, which led to the identification of 307 websites opened by three members of the organization. In addition, the records identified various complaints alleging that the websites were utilizing addresses and phone numbers for various individuals and businesses. One of the websites was using a police department's dispatch line as its contact phone number. This created a public safety issue for the Irvine Police Department because its dispatch line was inundated with complaints from the website's customers.

Throughout the investigation, HIS used BSA reporting to identify additional victims and websites. The supporting documentation assisted agents in connecting the suspects to the fraudulent activity because the suspects would utilize the same business name, phone numbers, bank accounts, and IP addresses on multiple accounts. HSI was able to use this information to obtain Federal search warrants into some of the email accounts, which positively identified the primary suspect behind the fraud. Utilizing the BSA data, agents were able to connect the defendants to more than 1,000 accounts that generated more than $1 million between December 2019 and April 2020 through 40,000 transactions from victims located throughout all 50 states and other countries.

The suspects were sentenced to a total of 31 years imprisonment. The U.S. Attorney's Office for the Middle District of Florida prosecuted the case.