Compilation of Award Recipient & Nominated Cases

AWARD RECIPIENT

Cybercrime – *United States Attorney's Office, Southern District of New York*

Over 100 Bank Secrecy Act (BSA) reports assisted in the investigation into a cryptocurrency fraud scheme, "OneCoin," that defrauded millions of victims around the world and resulted in billions of dollars in losses.

OneCoin Ltd. ("OneCoin") was founded in 2014. OneCoin marketed and sold a fraudulent cryptocurrency by the same name. OneCoin began operating in the United States in or around 2015. Between the fourth quarter of 2014 and the fourth quarter of 2016 alone, the scheme took in more than $4 billion from at least 3.5 million victims.

BSA reporting proved vital to this investigation. Specifically, through leads generated by BSA reporting, investigators were able to collect and analyze bank records, interview witnesses, and unravel a sprawling international fraud and money laundering scheme.

Analysis of the financial transactions involving one of the subjects, who was based in the United States, and his companies, revealed that the subject was one of the principal money launderers for the fraudulent scheme. The subject laundered over $300 million of OneCoin proceeds through U.S. and international bank accounts. The leads generated through BSA reporting enabled the Government to charge the subject, who was the first defendant to be charged in connection with the scheme.

In addition, BSA information revealed suspicious financial activity between several suspects and their businesses, including numerous transactions involving overseas bank accounts that were inconsistent with one of the company's reported business activities. BSA reporting also indicated that one of the subjects was involved in prepaid cards for OneCoin. Investigators also utilized the Egmont Program which provided valuable information that helped piece together the inner workings of this elaborate scheme.

This investigation resulted in more than a dozen arrests. OneCoin conspirators, including the co-founders of OneCoin, were charged in connection with their participation in the fraud scheme or related schemes to launder proceeds, defraud U.S. banks, and/or participate in extortion plots connected to the recovery of proceeds.

Nearly $100 million in assets from the scheme were seized, and forfeiture orders totaling approximately $1 billion were successfully obtained.

Notable sentences include a 20-year term of imprisonment for one of the co-founders, and a 10-year sentence for a former law firm partner based in the United States who was convicted of laundering $400 million in OneCoin proceeds. OneCoin leader and co-founder Ruja Ignatova was added to the FBI's Top Ten Most Wanted List in June 2022 and an award is being offered of up to $5 million for information leading to her arrest.

The OneCoin scheme was one of the largest fraud schemes that has ever been prosecuted by the United States Attorney's Office for the Southern District of New York.

Drug Trafficking Organization Activity – *United States Attorney's Office for the Western District of Washington*

While conducting surveillance on a drug trafficking organization (DTO), investigators identified a money courier. Based on Bank Secrecy Act (BSA) reporting, it was discovered that the subject had been making multiple, large, even numbered deposits at numerous financial institutions throughout the country.

Based on these findings, law enforcement began to investigate a money laundering organization that was moving illicit drug proceeds to Mexico for this DTO, along with many other DTOs throughout the country using funnel accounts opened at a particular financial institution. Investigators were able to identify a larger network of people engaged in the same activity by canvassing BSA reporting.

Scheduled BSA queries were created matching the typology of cash deposits and account holders seen throughout this investigation; these daily queries were essential to the investigation. FinCEN training sessions provided instrumental information on creating these queries. Each day, new filings would identify new deposits made as well as additional transactions made by known depositors and account holders. Supporting documents were requested and new subpoenas were issued for each filing to further track ongoing activity as well as attempt to identify new depositors. Supporting documents were instrumental to this investigation as photos and depositor identification was often recorded. In total, more than 4,700 FinCEN filings were reviewed during this investigation and more than 140 grand jury subpoenas were issued.

Eighteen people were indicted for their involvement in this money laundering organization. The grand jury returned a total of 97 counts against those 18 defendants, including an overarching conspiracy to commit money laundering and numerous substantive money laundering counts for concealment and international money laundering. Nine of those defendants were apprehended, have pled guilty, and have been sentenced. It was determined that this money laundering organization moved $17.4 million. A total of $256,215 in U.S. currency was seized during the investigation.

Fraud – *Environmental Protection Agency Criminal Investigation Division*

Bank Secrecy Act (BSA) reporting was crucial to the case development and successful prosecution of the biggest biodiesel and tax fraud schemes in the industry.

The conspiracy began in 2010, continued through 2018, and involved multiple fraudulent schemes. One scheme involved purchasing biodiesel from the east coast of the United States (which had been

produced by others who had already claimed the renewable fuel tax credit and Environmental Protection Agency (EPA) renewable identification numbers), exporting the fuel to foreign countries, then doctoring transport documents to disguise and import the biodiesel back to the United States as "feedstock." The company used this false feedstock paperwork to claim it was used to produce new biodiesel and support the filing of fraudulent claims for Internal Revenue Service (IRS) biofuel tax credits and EPA renewable identification numbers. Throughout the conspiracy the company fraudulently obtained millions of EPA renewable identification numbers that were then sold for approximately $65 million.

Another scheme involved two co-conspirators who colluded to purchase millions of gallons of biodiesel and rotate it through the U.S. shipping system to create the appearance that qualifying fuel was being produced and sold by the company. The company applied for and received over $300 million from the IRS for its claimed 2013 production and over $164 million for its claimed 2014 production. Evidence at trial showed that to further create the appearance of legitimate business transactions, the conspirators cycled over $3 billion of fraud proceeds in financial transactions through multiple bank accounts.

Together, the conspirators made false claims on the U.S. Government exceeding $1 billion utilizing a biodiesel company. BSA reporting was instrumental in identifying the fraud scheme and limiting the losses to $511 million. The investigators (including the EPA's Criminal Investigation Division, IRS Criminal Investigation, and Defense Criminal Investigative Service) were able to use the information to react and stop the additional claims of over $600 million from being paid by the IRS.

The prosecution led to the successful conviction of five individuals. In addition to prison sentences ranging from 6 to 40 years, the defendants were also ordered to pay significant restitution to the IRS.

The Department of Justice Tax Division prosecuted the case out of the District of Utah.

Human Trafficking/Human Smuggling – *Homeland Security Investigations*

In November 2019, Homeland Security Investigations (HSI) received information on alleged illegal activities being conducted by a business operating in several states. The allegations indicated the owner was involved in an ongoing criminal conspiracy to induce undocumented non-citizens to travel to the United States for the purpose of providing labor at grossly reduced wages.

Throughout the course of the investigation, investigators learned that the subject owned and operated several U.S.-based businesses as well as production factories in several states that were staffed by undocumented non-citizens. The owner used a broad network of undocumented non-citizen subcontractor work crews.

In 2019, the business had sales exceeding $53 million, and the company was on track to have sales exceeding $70 million for 2020. Analysis of financial records including Bank Secrecy Act reporting, revealed thousands of transactions through at least 10 business and personal bank accounts of the business owner.

Investigators estimated that approximately $15 million per year was being laundered through these accounts to include approximately $2 million in bulk U.S. currency per year from the illegal sales of controlled substances.

Conspiring with others to falsify and create fraudulent business records to support the loan applications, the suspect filed three applications for the Paycheck Protection Program and received approximately $700,000 in forgivable Federal loans.

The target company plead guilty to money laundering and bank/wire fraud. In addition, there were 21 administrative arrests, the seizure of over $13 million from bank accounts and over $400,000 in bulk U.S. currency, and the seizure of five vehicles totaling over $500,000.

The corporate entity was sentenced to three years of probation for knowingly conspiring to encourage and induce illegal aliens to remain in the United States, ordered to forfeit over $5 million of seized proceeds and was debarred from government procurement and non-procurement programs for a period of three years.

The United States Attorney's Office for the Southern District of Ohio prosecuted this case.

State and Local Law Enforcement – *Manhattan District Attorney's Office and New York Police Department*

Members of the New York City Police Department's Intelligence and Counterterrorism Bureau arrested a subject on New York State charges of soliciting or providing support for an act of terrorism, money laundering in support of terrorism, conspiracy, and criminal possession of a weapon.

This investigation began when investigators reviewed Bank Secrecy Act (BSA) information indicating an individual sent cryptocurrency to a known terrorist group. The financial information provided the investigation team with a window into what would turn out to be a complex terrorism financing network.

The subsequent investigation and evidence presented at the trial showed that the subject used cryptocurrency and more traditional financial services to finance and launder money for a Federally designated terrorist organization and a military training group. The majority of the investigation was further assisted by the discovery and review of additional BSA reporting that provided information on those financial institutions the network was utilizing.

In particular, the BSA information revealed that the subject sent and received numerous money transfers, converted several hundred dollars of cryptocurrency into prepaid cards, withdrew several hundred dollars of cryptocurrency from ATMs, and sent and received thousands of dollars of cryptocurrency using exchanges and a non-custodial wallet all in furtherance of the terrorist group's efforts in a particular country.

Over the course of the investigation, law enforcement executed numerous electronic warrants on the subject's email and cloud accounts. The review of these accounts revealed evidence of the subject's major role as a financier and launderer for the terrorist group.

The subject was charged with soliciting or providing support for an act of terrorism, money laundering in support of terrorism, conspiracy, and criminal possession of a weapon. After a three-week jury trial, the subject was convicted on all counts, representing the first terrorism and cryptocurrency financing case and conviction in New York State history. The subject was sentenced to 18 years in prison and five years of post-release supervision.

The Manhattan District Attorney's Office prosecuted this case.

Transnational Criminal Organization Activity – *United States Attorney's Office, Northern District of Georgia*

This investigation began after law enforcement received a referral from a financial institution concerning an employee who was caught recording customers' information and accessing their accounts without authorization.

Investigators discovered that the employee had previously been fired from another financial institution for similar conduct. The investigation revealed the subject orchestrated the withdrawal of $120,000 from a customer's account. The subject then recruited co-conspirators to pose as the victim and withdraw the funds via cashier's checks, using false identity documents in the victim's name. Those checks were issued to and cashed by co-conspirators.

Through a review of bank records for accounts controlled by the primary subject and their co-conspirators involved in the bank fraud scheme, investigators learned that many of the individuals had received large deposits into their accounts from additional fraud victims.

The subject and nine others were indicted on charges of money laundering, bank fraud and aggravated identity theft. The primary subject agreed to cooperate, and law enforcement continued to investigate the conduct, which led to additional indictments against more than 30 conspirators.

This large-scale fraud and money laundering operation targeted citizens, corporations, and financial institutions throughout the United States and abroad. Business email compromise schemes, romance fraud scams, and retirement account takeover schemes duped hundreds of victims into sending substantial amounts of money to the defendants and their co-conspirators. Some of these schemes targeted elderly victims and depleted the victims' entire life savings, including retirement funds.

The defendants and their co-conspirators facilitated the fraud schemes by receiving and distributing fraudulent funds throughout the United States and other countries. The defendants created multiple sham companies that did not have physical premises, earn legitimate income, or pay wages to employees. To facilitate the receipt and distribution of the fraud proceeds, the defendants opened business bank accounts for their sham companies, as well as personal bank accounts using false identities and victims' identities. After the fraud proceeds were deposited into these accounts, the proceeds were quickly withdrawn and distributed to members of the conspiracy, making it virtually impossible for the banks to recall the funds when the fraud was discovered.

Almost 1,000 Bank Secrecy Act reports were used in the investigation and assisted with piecing together the puzzle of this extensive fraud scheme. The criminal organization that perpetrated the fraud was organized and sophisticated, and BSA data allowed the investigative team to pinpoint relevant activity. The team reviewed records for more than 300 bank accounts during the course of the investigation, and agents interviewed approximately 150 victims.

This expansive investigation led to the convictions of 40 defendants, with sentences ranging from 3 to 216 months' incarceration.

Corruption – *Homeland Security Investigations*

Law enforcement initiated an investigation into an international money laundering organization responsible for laundering illicit proceeds obtained by politically exposed persons (PEPs). Utilizing a scheme comprised of loan contracts, credit assignments and secondary market currency exchanges, the PEPs embezzled approximately $1.2 billion from a Southern American country into financial institutions throughout the world. The PEPs utilized third-party money laundering organizations that included currency brokers and attorneys to layer and conceal the currency to disguise the true origins of the funds.

The scheme involved PEPs that embezzled large amounts of currency by exploiting their country's restricted foreign exchange market and abusing their official positions by entering favorable loan contracts with an oil industry company. The loan contracts allowed for funds to be loaned to the company and then be paid back in foreign currency at favorable exchange rates. The foreign currency was then exchanged on the secondary market by the PEPs, generating inflated returns.

Throughout this investigation, Bank Secrecy Act reporting was instrumental in allowing case agents to trace the flow of funds through financial institutions domestically and abroad. Specifically, the use of 314(a) and Egmont information provided the investigating agents the ability to trace the illicit proceeds of the illegal activity globally.

Utilization of the Egmont Program provided information on targets of investigation in 38 countries and, as a result, investigating agents were able to identify and develop evidence that led to seizures totaling $268 million from financial institutions.

The information received by case agents was used to trace the global movements of ill-gotten gains derived from the criminal activity and provide crucial evidence used in support of criminal indictments against PEPs, third-party money launderers, and other co-conspirators.

The United States Attorney's Office for the Southern District of Florida prosecuted this case.

NOMINATED CASES

Fraud – *Arlington County, VA Police Department*

This case involved the use of stolen credit card numbers used to purchase gift cards, expensive luxury goods, and other items at various retailers throughout the Arlington, Virginia area. During the course of the investigation, a single Bank Secrecy Act report provided insight into a complex fraud scheme involving a business, its owners, and their associates. The fraudulent activity involved thousands of payment cards and resulted in significant losses to various financial institutions.

Three of the four defendants were convicted and sentenced to 10 years' imprisonment along with 5 years of supervision upon release. The fourth defendant received a prison sentence of 14 years. All defendants were ordered by the court to pay a total of more than $500,000 in restitution to victims. The United States Attorney's Office for the Eastern District of Virginia prosecuted this case.

Fraud – *United States Attorney's Office for the Western District of Texas*

Based on a review of numerous Bank Secrecy Act (BSA) reports, the Federal Bureau of Investigation, Internal Revenue Service-Criminal Investigation, and the United States Attorney's Office for the Western District of Texas launched an investigation into a complex financial scheme involving a subject who was the recipient of funds from two non-profit charity organizations.

Specifically, the defendant, who previously served as the Small Business Administrator, and his coconspirator operated a charity where they solicited donations into that charity to be used to establish an apprenticeship program to help low-income youth get critical job training and skills. The defendants stole much of these funds for personal use themselves through direct and indirect payments to themselves, using the charity's credit cards for personal expenses, and payments to friends and family members. To further conceal their scheme, the co-conspirators funneled payments through third parties who would funnel the money back to the subjects. They used false invoices and tax documents to make the payments appear legitimate and to further hide the ultimate recipients of the charitable funds.

BSA reporting and supporting documents helped initiate the investigation. From those leads, law enforcement obtained the related bank account information that helped unravel the scheme.

Both defendants were indicted by a grand jury and later convicted of numerous fraud and tax violations. The first defendant received a term of imprisonment of 20 months, a fine of $100,000, 3 years of supervised release, and court ordered restitution of over $900,000. The second received 5 years of probation with 10 months of imprisonment as a condition of that probation, a fine of $100,000, and a total court ordered restitution of over $1 million.

Fraud – *Internal Revenue Service–Criminal Investigation*

This matter involves an investigation into a bond fraud scheme perpetrated by an individual and his companies.

The defendant falsely claimed to be experienced in and able to provide surety bond and other financial guarantees for large-scale projects and told victims he would assist them in obtaining

financing for their projects via his various companies. To make the scheme appear legitimate, the subject hijacked corporate filings of other companies and created fake employees and fake accounts for underwriters and banks.

From its inception and throughout the investigation, Bank Secrecy Act information as well as FinCEN's 314(a) Program were instrumental in identifying leads, assisting in determining the lead's value, and focusing efforts to efficiently locate and determine the best evidence.

The defendant was sentenced to 110 months in federal prison for defrauding victims out of more than $5 million by purporting to sell bonds for large-scale construction and other projects, and for evading the payment of more than $1.2 million in taxes. He was also ordered by the court to pay over $8 million in restitution. The United States Attorney's Office for the Central District of California prosecuted this case.

Fraud – *Internal Revenue Service–Criminal Investigation*

The Internal Revenue Service–Criminal Investigation, the Federal Bureau of Investigation, and the United States Postal Service investigated subjects for stealing over $40 million by using a company to make false and fraudulent claims on the proceeds of securities fraud class action settlements and U.S. Securities and Exchange Commission (SEC) enforcement action settlements.

To substantiate the false claims, the defendants created fraudulent brokerage and other financial documents to provide to claims administrators. The subject and co-defendants then transferred the fraudulently obtained funds into accounts they controlled.

Bank Secrecy Act reporting from multiple financial institutions provided insight into the movement of millions of dollars between seemingly unrelated bank accounts for no apparent economic purpose.

The primary subject was found guilty of conspiracy to commit wire fraud, mail fraud, and money laundering, and was sentenced to 10 years in prison and ordered by the court to pay $31.2 million in restitution. The United States Attorney's Office for the Eastern District of Pennsylvania prosecuted this case with trial support from the United States Attorney's Office for the District of New Jersey.

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

This matter involves an investigation and prosecution of the fraudulent sale of real estate. In particular, the defendants in the scheme falsely listed properties for sale on real estate listing services, held open houses, and collected money from would-be buyers through the operation of corrupt escrow firms. The defendants then accepted numerous down payments—and sometimes the full purchase price—for the not-for-sale homes. When victims figured out what happened and demanded their money back, the defendants changed aliases, created fake businesses and addresses, and began the scheme at a new location.

Bank Secrecy Act information was a critical component in this investigation as it assisted with identifying subjects, leads, financial accounts, and victims.

The co-conspirators collected more than $11.7 million from 750 or more victims as part of their scheme. The scheme caused more than $6 million in losses to nearly 400 victims. All three charged defendants pled guilty and were sentenced to varying terms of imprisonment. The court ordered the defendants to pay over $5 million in restitution to over 400 victims. The United States Attorney's Office for the Central District of California prosecuted this case.

Fraud – *Internal Revenue Service–Criminal Investigation*

The Internal Revenue Service – Criminal Investigation received an anonymous tip regarding a pharmacist and CEO of a medical company who was engaged in check kiting. The investigation revealed the subject was responsible for paying the company's taxes, making the company's financial decisions, and authorizing financial transactions. For 8 years, he evaded paying over $6 million in Federal payroll taxes.

Through a review of Bank Secrecy Act reporting, law enforcement discovered significant movement of money from the subject's business accounts to his personal account.

The subject pleaded guilty to tax evasion and was sentenced to 24 months in prison, followed by 24 months of supervised release, and ordered by the court to pay $6,058,980 in restitution. The United States Attorney's Office for the District of Minnesota prosecuted this case.

Fraud – *Food and Drug Administration, Office of Criminal Investigations*

This investigation involved a network of illicit online pharmacies and call centers importing unapproved misbranded narcotics into the United States from foreign countries.

During the course of the investigation law enforcement identified multiple subjects throughout the United States and other foreign jurisdictions. Investigators also identified a high-level operator in the organization who was involved in the supply of drugs, shipping logistics, and financial accounting.

Bank Secrecy Act (BSA) reporting was invaluable in the identification and analysis of this significant criminal enterprise. Overall, the investigation identified approximately 200,000 financial transactions totaling over $33 million.

Through collaboration with various Federal, state, local, and international law enforcement agencies, this investigation led to the identification, arrest, and prosecution of nine network operators across the globe including the extradition of three foreign nationals. Law enforcement seized over $2 million in illicit assets. The United States Attorney's Office for the District of Vermont prosecuted this case.

Fraud – *New Jersey State Police*

The New Jersey State Police opened an investigation into a large-scale check fraud and money laundering operation. During the course of the investigation, law enforcement analyzed Bank Secrecy Act reporting. This reporting provided vital substantive information that led to the discovery of the fraud and money laundering network and additional associates, aided law enforcement in deciphering co-mingled funds, and identified vulnerabilities of the extensive illicit financial network.

Evidence obtained revealed over 1,988 stolen checks totaling more than $9.7 million dollars, check making software, fraudulent tax documents/paystubs, and over 1,000 personal identifying information items including credit cards, drivers' licenses, Social Security cards, and numerous bank account/routing numbers.

Law enforcement charged 35 co-defendants across multiple states, including arresting the lead defendant. The law enforcement actions disrupted the criminal network and prevented over $9 million in additional stolen funds and fraudulent checks from entering the banking system.

The Atlantic County New Jersey Prosecutor's Office prosecuted this case.

Fraud – *Internal Revenue Service–Criminal Investigation*

The Internal Revenue Service-Criminal Investigation investigated a suspected ringleader of a large betting ring spread across several casinos who was alleged to be involved in money laundering activities for other parties and gambled using solicited investment money from victims.

Information derived from over 1,000 Bank Secrecy Act reports indicated the subject was a professional gambler who received money from third parties to fund legal gambling.

A grand jury investigation found criminal violations of wire fraud and tax fraud. The investigation obtained evidence that the defendant solicited over $10 million in investment proceeds. The subject claimed to the investors that he invested their funds in the stock market, earning profitable returns on sports wagers placed on the major professional sports. Further, the subject used over $2 million of the victim-investor's funds on personal expenses such as vacations, clothing, jewelry, and luxury vehicles.

The subject was charged and pled guilty to federal wire fraud and tax fraud and was sentenced to 28 months of imprisonment and ordered by the court to pay $7,106,888 in restitution to his victims. The United States Attorney's Office for the Northern District of Illinois prosecuted this case.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations received information on a subject falsely claiming to be employed by the Department of Homeland Security, and who used this apparent position of authority to defraud several undocumented non-citizens. Specifically, law enforcement learned the subject portrayed herself to be a U.S. Citizenship and Immigration Services (CIS) employee, and defrauded numerous undocumented noncitizen victims and their family members by falsely representing that she would process their immigration applications for a substantial fee. The defendant's victims provided her with the documentation required to file and adjust their immigration status. However, she was not an employee of CIS and never took any actions to adjust the victims' status. Once the victims became aware of the fraud and complained, the perpetrator would threaten them with deportation.

During the investigation, Bank Secrecy Act reporting was valuable in providing information on the unusual movement of funds being conducted by the subject and also identified several victims who were later interviewed. Through these victim interviews, law enforcement found that the subject defrauded over 30 individuals.

The subject was charged with wire fraud and impersonation of a U.S. employee, sentenced to 87 months' imprisonment, and ordered by the court to pay $123,000 in restitution and an additional $19,000 in a money judgment. The United States Attorney's Office for the Western District of Texas prosecuted this case.

Fraud – *Department of Justice, Office of the Inspector General*

The Department of Justice Office of the Inspector General and the United States Postal Inspection Service jointly investigated a government contractor deputized with law enforcement authorities who was conducting a significant romance scam fraud scheme. The Department of Justice Office of the Inspector General, Cyber Investigations Office; the Federal Bureau of Investigation; and the Prince George's County, Maryland Police Department assisted with this investigation. The United States Attorney's Office for the District of Maryland prosecuted this case.

According to the factual statement in support of the guilty plea, from in or about October 2015 through in or about July 2021, the subject transmitted monetary instruments and funds to a place outside of the United States with the intent to carry out a specified unlawful activity. Specifically, the subject accepted money from at least ten romance scam victims and, after retaining a percentage of the proceeds as a fee, transferred the remaining funds to co-conspirators in Nigeria. The subject laundered more than $1.4 million as a result of the conspiracy.

Bank Secrecy Act reporting was critical in identifying the numerous bank accounts as well as the victims the subject was using as part of the fraud scheme. Through interviewing the victims, law enforcement found shared unique commonalities, such as meeting the subject online and the subject claiming to be a deployed member of the U.S. Armed Forces; every victim of the romance scam provided, or attempted to provide, money to the subject with whom they were speaking; and many of the victims were elderly.

The subject pleaded guilty to one count of money laundering conspiracy and, on April 11, 2024, was sentenced to 33 months of imprisonment, 3 years of supervised release, and ordered to pay over $1,350,000 in restitution.

Fraud – *Internal Revenue Service–Criminal Investigation*

The Internal Revenue Service – Criminal Investigation, and the United States Attorney's Office for the Southern District of Georgia investigated an international fraud scheme misdirecting more than 30 million dollars in charitable donations intended for Christian outreach in China. Investigators utilized Bank Secrecy Act reporting to identify domestic and international bank accounts, both at the center of the scheme.

A civil forfeiture complaint was filed on numerous assets associated with the scheme, including privately held stock with a value of approximately $850,000; 11 life insurance policies with a total value of approximately $380,547; $28,581 in cash seized from 7 bank accounts across the United States; $18,673 in cash seized from a basement; and silver bars, silver coins, and rare coins dating back to the 1880s. The total value of forfeited assets was approximately $1,277,801.

A federal grand jury returned a 37-count indictment against the subject. The indictment alleged multiple counts of wire fraud, international concealment of money laundering, money laundering

involving transactions greater than $10,000, and failure to file a foreign bank account. As of December 2024, the defendant remains an international fugitive.

Fraud – *New York State Police*

The New York State Police received a request for assistance regarding fraudulent activity involving a local company's business operations. Investigators discovered that after the departure of the company's business manager, the owner took over the handling of the company's daily operations. The owner noticed that the company paid the payroll manager significantly more than their hourly rate.

Review of Bank Secrecy Act reporting identified large payroll deposits and numerous cash withdrawals from over four different financial institutions. In addition, the financial activity indicated the suspect was living well beyond their means. Audit findings showed the total amount embezzled from the company over a 4-year period was more than $1 million.

The subject was convicted of grand larceny and falsifying business records and sentenced to 5-to-15 years in prison, followed by 2 years of post-release supervision. The Cortland County New York District Attorney's Office prosecuted this case.

Fraud – *United States Secret Service*

This investigation originated from a complaint filed through the Internet Crime Complaint Center (IC3) by a victim identifying an attempted business email compromise (BEC) scheme. Specifically, the victim alleged that a company received a fraudulent invoice by email for "Business Development & Consulting Services" instructing payment to be made to an individual (and not a business). The email also provided Automated Clearing House information for a bank account that listed the beneficiary as the same individual. The company identified the invoice as fraudulent and did not make any payments but still reported the information.

Law enforcement executed arrest and search warrants, ultimately arresting 10 subjects. An eleventh subject self-surrendered, and law enforcement arrested the twelfth and final subject at an airport. Law enforcement seized three luxury vehicles and approximately $140,000 in cash, along with approximately $125,000 in cryptocurrency.

A grand jury charged the defendants with conspiracy to commit money laundering, conspiracy to commit bank fraud, and one with aggravated identity theft. All defendants, except one who died in an accident prior to a plea hearing, pled guilty to charges of either conspiracy to commit money laundering or bank fraud.

Based on the complaint, investigators conducted database searches on the account, name, and address, including queries of Bank Secrecy Act (BSA) Information. The initial investigation found multiple subjects using fraudulent identities to open bank accounts. Victims of various fraud schemes, including BEC, romance scams, social media scams, and COVID relief fraud sent over $2 million to these accounts.

Investigators conducted extensive and recurring searches of related identifiers and reviewed approximately 347 BSA Reports. The reports were instrumental in helping to identify and link the subjects and their money laundering activities.

Investigators analyzed, in total, over 252 bank accounts related to 12 subjects for money laundering activity and found that these accounts received over $19 million from victims. Investigators also interviewed over 50 victims (individuals, businesses, and government agencies) and verified approximately $9.1 million stolen through this fraud scheme.

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

Fraud – *United States Secret Service*

The United States Secret Service, together with the Food and Drug Administration-Office of Criminal Investigations; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and the Cape Coral Police Department investigated an individual believed to be connected to seized packages containing prescription drugs, drug precursors, and controlled substances. The matter was prosecuted by the United States Attorney's Office for the Middle District of Florida, and assisted by the United States Postal Inspection Service, Homeland Security Investigation, the Drug Enforcement Administration, the Florida Highway Patrol, and the Pasco Sheriff's Office. The investigation resulted in a conviction and one of the largest pill seizures in Southwest Florida.

BSA information was instrumental at every stage of this investigation and was principal in identifying the multiple layers of fraud and account activity. Law enforcement was able to readily identify accounts at multiple financial institutions and cryptocurrency wallets linked to the suspected drug activity and allowed investigators to identify a scheme to defraud at least two financial institutions.

Investigators connected BSA data together with other pieces of evidence demonstrating the individual was running a large-scale drug manufacturing operation. Based on this information, law enforcement executed a search warrant of the subject's residence and found a pharmaceutical grade industrial tablet pill press; over 2,000 counterfeit oxycodone pills that contained fentanyl packaged for delivery; a five-gallon bucket containing over 30 pounds of counterfeit Xanax pills (which translated to over 45,000 counterfeit pills); and other pill making materials and equipment.

The subject was convicted and sentenced to 21 years and 10 months in federal prison for possession of a controlled substance (fentanyl) with the intent to distribute it, possessing counterfeit drugs for sale, possessing equipment used to manufacture counterfeit drugs, possessing a firearm as a convicted felon, and bank fraud. The court also ordered the subject to pay a $500,000 fine, forfeit over $970,000 to the United States, and make full restitution to victims for his bank fraud.

Fraud – *Internal Revenue Service–Criminal Investigation*

The Internal Revenue Service-Criminal Investigation, the Federal Bureau of Investigation, and the United States Postal Inspection Service investigated an individual suspected of operating an unregistered money services business. The perpetrator owned and operated several automatic teller machines (ATMs) and provided services involving exchanging cash for the digital currency Bitcoin.

As part of the investigation, more than 600 Bank Secrecy Act reports played a crucial role in identifying more than 50 victims, multiple bank accounts, and millions of dollars in assets. The victims were defrauded as a result of various online scams, such as romance scams, lottery scams, grandparent scams, and advanced fee scams.

The subject laundered over $10 million in proceeds from these scams and other internet frauds by exchanging U.S. dollars for bitcoin. The defendant was arrested and charged with participating in a conspiracy to operate an unlicensed money transmitting business. He received a sentence of 96 months, was ordered to pay a fine of $40,000, and forfeited $5.2 million.

The National Cryptocurrency Enforcement Team and the Department of Justice, Tax Division provided valuable assistance in the case. The United States Attorney's Office for the District of New Hampshire prosecuted this case.

Fraud – Department of *Housing and Urban Development, Office of Inspector General*

The United States Department of Housing and Urban Development, Office of Inspector General; the Federal Bureau of Investigation; and the Federal Housing Finance Agency, Office of Inspector General investigated 12 individuals for submitting false information on mortgage applications in order to fraudulently obtain lender approval.

The investigation originated from several Bank Secrecy Act reports filed by a mortgage company on two individuals. During the investigation, law enforcement discovered additional real estate brokers who, along with the initial subjects, were involved in a separate scheme, to defraud a real estate company of unearned commissions. The co-conspirators falsely claimed to represent homebuyers as their selling agents to receive commissions from the home sales.

In all, 12 defendants were charged for their roles in the two schemes. Eleven defendants pled guilty, and the primary subject was found guilty on all charges after a jury trial. Over 110 primarily Federal Housing Administration (FHA)-insured mortgages for approximately $27 million were issued based on fraudulent submissions uncovered in the investigation. Approximately $1.5 million in claims to FHA resulted due to borrowers not paying their mortgages. Approximately $480,000 in unearned commissions were paid by the real estate company. The United States Attorney's Office for the Northern District of Georgia prosecuted this case.

Fraud – *Internal Revenue Service–Criminal Investigation*

Internal Revenue Service-Criminal Investigation, together with the Federal Bureau of Investigation and the United States Attorney's Office for the Southern District of Indiana, investigated alleged financial improprieties of an individual who was hired to assist with the start-up and operation of a trucking company. The trucking company authorized the subject to use the company's funds for company expenses and to pay himself a salary.

By analyzing over 60 Bank Secrecy Act (BSA) reports, law enforcement determined the subject had committed fraud and money laundering. BSA information was a critical tool in identifying financial transactions, accounts, and a multitude of assets intertwined in the scheme. This information helped the team to efficiently secure financial records and evidence in support of probable cause for search and seizure warrant, as well as a 19-count criminal indictment for violations including wire fraud, money laundering, and mail fraud.

Law enforcement arrested the subject, and he pled guilty to one count of wire fraud and one count of money laundering and was sentenced to 72 months' imprisonment, 3 years of supervised release, and ordered by the court to pay more than $14 million in restitution to his victims.

The United States Attorney's Office for the Southern District of Indiana prosecuted this case.

Fraud – *Homeland Security Investigations*

Homeland Security Investigations (HSI) investigated an individual for providing false information in order to obtain Economic Injury Disaster Loans (EIDL) from the Paycheck Protection Program (PPP). The United States Attorney's Office for the Eastern District of Michigan prosecuted this case.

This matter originated from *Operation Regulator*, an HSI-led initiative to investigate organizations, networks, and individuals that defrauded the government by exploiting the PPP and Small Business Administration (SBA) EIDL program under the CARES Act. *Operation Regulator* leverages authorities, tools, investigative techniques, and intelligence capabilities, including Bank Secrecy Act information.

Throughout the course of this particular investigation, law enforcement learned a subject applied for $963,000 in PPP and EIDL loans referencing fictitious businesses and employees. As a result, the subject received 13 loans totaling over $850,000.

Law enforcement charged the subject with wire fraud and bank fraud. The subject pled guilty to one count of wire fraud. As part of the plea, the subject agreed to a personal forfeiture money judgement of $851,963 and was sentenced to 27 months incarceration with two years of supervised release and ordered to pay $851,963 in restitution.

To date, *as part of Operation Regulator*, HSI has initiated over 35 criminal investigations of companies and individuals who illegally obtained PPP loans through fraud and/or used the funds for unauthorized purposes. Collectively, these suspects defrauded the United States government of many tens of millions of dollars. *Operation Regulator* has resulted in the seizure of nine bank accounts worth approximately $2.6 million, two indictments, seven search warrants, and an affidavit of interest against a property worth approximately $400,000.

Corruption – *Homeland Security Investigations*

Homeland Security Investigations investigated a foreign financial institution that was specifically created to launder funds and pay bribes on behalf of several Politically Exposed Persons (PEPs) who embezzled large amounts of currency from their country's government.

In particular, the PEPs conspired with complicit bankers that had international access to sophisticated financial structures and foundations to further launder and conceal the beneficial ownership of funds totaling more than $1 billion. The reach of the organization affected the financial infrastructure of many countries worldwide.

The primary target of the investigation had access to the country's official currency rate through state-sponsored contracts. The country's Appropriations Committee awarded these contracts, and the head of the country's Treasury made corresponding payments.

With the assistance of Bank Secrecy Act reporting, law enforcement obtained evidence to support a $1 billion judgement, of which it successfully forfeited $257,579,943. In addition, investigating agents seized three properties valued at $15 million, show horses valued at $2 million, 10 vehicles valued at $1 million, and luxury watches with a value of $1.4 million.

A grand jury indicted two subjects, who were later convicted of conspiracy to launder monetary instruments and sentenced to a total of 25 years' imprisonment. The United States Attorney's Office for the Southern District of Florida prosecuted this case.

Corruption – *Homeland Security Investigations*

Homeland Security Investigations received information regarding embassy personnel who were embezzling funds from their foreign government and laundering the proceeds through a series of U.S. based shell companies. The scheme was initiated by a citizen and national of the foreign country with diplomatic status in the United States.

In just under eight months, members of the conspiracy embezzled over $1.5 million in government funds by submitting fake invoices for medical services that were never provided. Members of the conspiracy obtained additional funds by creating fake patient profiles in the health office's computer systems.

The fraud scheme was discovered and ultimately disrupted when members of the conspiracy overdrew from the embassy bank account. To conceal their criminal activity, members of the conspiracy attempted to return approximately $430,000 in stolen funds via check deposit. When the checks bounced, the foreign government launched an internal investigation into the embassy personnel.

The chief conspirator was arrested and charged by their foreign government with fraud against the government and money laundering. The subject was removed from the United States and arrested by their country's authorities.

Three co-conspirators pled guilty to one count of conspiracy to commit money laundering. One was sentenced to 24 months in prison and ordered by the court to forfeit $1.4 million. The second was sentenced to 12 months and a day in prison and ordered by the court to forfeit $1.4 million. The third was sentenced to 36 months in prison and order by the court to forfeit $1.5 million.

Bank Secrecy Act reporting was instrumental to investigators' success by identifying bank accounts linked to the suspected shell companies. Law enforcement obtained additional financial records pursuant to subpoenas, 314(a) requests, and Egmont requests. The U.S. Department of Justice's Criminal Division – Money Laundering and Asset Recovery Section prosecuted this case.

Corruption – *Department of Veterans Affairs, Office of Inspector General*

Based on a Hotline tip, the Department of Veterans Affairs (VA), Office of Inspector General opened an investigation into a VA employee who had been absent on official leave for several months and was responsible for over $300,000 in purchase card transactions despite not working. The investigative team pursued this lead and determined that the employee's purchase card transactions primarily involved a specific group of vendors. Subsequent analysis identified additional subject vendors, facilities, and VA employees involved in a larger scheme.

Bank Secrecy Act reporting assisted investigators in identifying several main defendants. Due to multiple subjects (VA employees and vendors) and the scale of the fraud scheme, law enforcement utilized the 314(a) Program to identify all accounts associated with the subject vendors and VA employees. The results of their 314(a) request yielded over 130 previously unknown accounts.

This fraud scheme identified vendors who paid kickbacks/bribes to VA employees in exchange for purchase orders and service contracts where the prices of supplies were grossly inflated, partially fulfilled, or not fulfilled at all, and contracted services which were not completed or completed using existing VA staff. The vendors charged in this case were responsible for over $37.6 million in purchase card orders and service contracts with the VA. Other aspects of this investigation focused on Service-Disabled Veteran-Owned Small Business fraud.

In total, this complex, multi-year, multi-jurisdiction investigation culminated with 19 defendants being charged, resulting in one pre-trial diversion, 18 guilty pleas, over 208 months of imprisonment, 606 months of probation/supervised release, $15,000 in fines, and over $9.7 million in restitution to the VA. Administratively, the investigation realized 27 suspensions, 11 debarments, and 15 employee terminations/resignations.

The United States Attorney's Office for the Southern District of Florida and the United States Attorney's Office for the Eastern District of Pennsylvania prosecuted this case.

Drug Trafficking Organization Activity – *Drug Enforcement Administration*

This matter involved a former Mexican law enforcement official who took millions of dollars in bribes from a Drug Trafficking Organization (DTO) and enabled transportation of one million kilograms of cocaine into the United States. The official utilized numerous shell companies to carry out the money laundering operation. Through the use of the 314(a) Program and the Egmont Program, law enforcement discovered additional account activity, both domestic and international.

Following a four-week trial, a jury convicted the defendant of engaging in a continuing criminal enterprise, international cocaine distribution conspiracy, conspiracy to distribute and possess, intent to distribute cocaine, and making false statements. The court sentenced him to over 38 years' imprisonment and ordered the defendant to pay a $2 million fine for his decade-long assistance to the DTO.

The United States Attorney's Office for the Eastern District of New York prosecuted this case.

Transnational Criminal Organization Activity – *Bureau of Alcohol, Tobacco, Firearms, and Explosives*

Based on a tip, the Bureau of Alcohol, Tobacco, Firearms, and Explosives launched an investigation into the attempted purchase of more than 500 high caliber assault rifle parts. Investigators obtained Bank Secrecy Act (BSA) reporting, which was crucial in identifying large money movements conducted by a known transnational criminal organization to an individual specializing in high-caliber and belt-fed firearms.

Law enforcement's continued use of BSA data identified additional bank accounts, firearms-related transactions, deposit locations, additional subjects of interest, and other important identifiers for network targets.

This investigation resulted in six indictments as well as the seizure of six assault rifles, more than 250,000 rounds of assault rifle ammunition, and more than $300,000 worth of weapons parts and kits used to assemble several high-powered machine guns bound for the transnational criminal organization's leadership. The indictments charged all six defendants in a conspiracy to violate export administration regulations that restrict the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to the foreign policy or national security of the United States.

The primary subject pled guilty to conspiracy to violate export regulations and conspiracy to commit money laundering and was sentenced to 57 months imprisonment. The United States Attorney's Office for the Central District of California prosecuted this case.

Transnational Criminal Organization Activity – *Internal Revenue Service-Criminal Investigation*

The Internal Revenue Service-Criminal Investigation investigated three individuals engaged in an investment fraud scheme targeting elderly individuals. As part of the scheme, telemarketing boiler rooms were used to contact victims by telephone. The perpetrators cold-called the victims and persuaded them to "invest" money under various false pretenses, promising guaranteed short-term, no-risk returns.

In reliance on the false representations, the victims sent funds to various shell company bank accounts controlled by the primary perpetrator. Instead of investing the funds, the subjects used them to support personal expenses or, wired them to various overseas corporate bank accounts controlled by other co-conspirators.

Bank Secrecy Act reporting was an important tool as law enforcement used it to identify various bank accounts being utilized by the primary subject and established that these accounts were linked to shell companies.

In total, this investigation resulted in the guilty pleas of the three subjects, court ordered restitution of more than $16 million, and a combined total sentencing of 156 months in prison.

The United States Attorney's Office for the Southern District of New York prosecuted this case.

Transnational Criminal Organization Activity – *Homeland Security Investigations*

Following a seizure at an airport mail facility of two shipments containing approximately 200 assault rifle weapon parts, Homeland Security Investigations opened an investigation into a transnational criminal organization (TCO). Both U.S. and international law enforcement officials conducted an International Controlled Delivery (ICD).

The ICD resulted in law enforcement's seizure of over 2,000 firearms, 500,000 rounds of assorted caliber ammunition, multiple mortar and artillery rounds, 49 hand grenades, 15 silencers, 88 kilograms of gun powder, one anti-aircraft artillery approximately $424,000 in mixed currency, fiver vehicles and the arrest of 44 international citizens and three US citizens for weapons violations. Bank Secrecy Act information was essential in identifying members of the TCO.

In total, this investigation resulted in over 40 arrests and the execution of over 70 search warrants. The efforts of law enforcement led to the dismantling of this world-wide weapons trafficking organization. The United States Attorney's Office for the Southern District of Florida prosecuted this case.

Operation Patagonia Express resulted in the largest law enforcement seizure of illicit firearms and ammunition in a South American country's law enforcement history.

Transnational Criminal Organization Activity – *Internal Revenue Service–Criminal Investigation*

This investigation involved a large-scale money laundering organization (MLO) operating both licensed and unlicensed check cashers as well as registered money services businesses, which the subjects used to conduct transactions derived from illicit proceeds from drug trafficking, wire fraud, bank fraud, identity theft, employment tax fraud, and criminal immigration violations.

The investigation found that over a 3-year period, the subjects cashed more than $290 million in checks against shell companies related to the construction industry. The co-conspirators allowed their customers to avoid financial records from being traced directly to them. This allowed the customers to commit other illicit activities without being reported, including off-the-books labor, tax evasion, and other crimes.

BSA searches on all known conspirators allowed investigators to identify the magnitude of the scheme. In total, over 1,000 BSA reports assisted with piecing together the puzzle of illicit activity.

Law enforcement conducted search, seizure, and arrest warrants that led to the arrests of two of the primary subjects, the seizure of over $1.3 million in cash, and the acquisition of significant evidence of additional co-conspirators in the scheme. The United States Attorney's Office for the District of New Jersey prosecuted this case.