Summary of Nominated Cases

State and Local – *San Jose Police Department*

As part of a murder investigation, the San Jose Police Department was reviewing video surveillance footage which showed an unknown suspect in an automobile. Investigators eventually identified the suspect, but could not find a link between the suspect and the vehicle.

They turned to Bank Secrecy Act records and found that the suspect paid $10,000 in currency for the purchase of an unregistered vehicle that matched exactly the description of the car in the video surveillance. Additionally, the vehicle was never registered under the suspect's name, but instead that of a straw purchaser.

The subject was arrested for murder and conspiracy to commit murder.

COVID-19 – *United States Secret Service*

The U.S. Secret Service (USSS) disrupted an attempted $317 million fraud on a foreign government by an individual trying to sell 50 million non-existent facemasks. Through his company, the subject agreed to act as a middleman in exchange for a cut of the sales price. The negotiated sales price for these masks was more than 500 percent higher than the previous normal market value for N-95 masks.

A financial institution contacted the USSS after a review of the account application revealed multiple errors and red flags, including an incorrect email address, a newly established company, a medical equipment supplies telemarketer, and an address that returned to a United Parcel Service storefront. The USSS then reached out to FinCEN's Rapid Response Team for help in contacting the foreign government and freezing the $317 million transaction.

COVID-19 – *Federal Bureau of Investigation*

A New Jersey man was charged with using other individuals' personal identification information to obtain unemployment insurance benefits created under the federal Coronavirus Aid, Relief, and Economic Security Act (CARES Act). A single IP address was used to submit unemployment insurance benefits claims on behalf of approximately 20 individuals to the State of New York. Many of these claims were in the names of individuals located in Texas and the defendant directed the benefits to be sent to locations in New Jersey. However, investigators discovered that the subject was associated with the IP address as well as a telephone number used to make some of the claims.

Analysis revealed positive results from a cell phone number that was used in one of the several dozen fraudulent claims. Additional results identified purchase of a vehicle in excess of $10,000 from which the investigators were able to identify the subject. Agents issued subpoenas on internet service providers for IP subscriber information, and several banks for documentation to corroborate that the subject was the perpetrator. Addresses for search warrants were obtained and corroborated by physical surveillance conducted by the case agents.

The subject was observed using an unemployment insurance benefits debit card to make a withdrawal from an ATM. The claims made using the IP address have resulted in more than $400,000 in actual losses and more than $600,000 in potential losses.

COVID-19 – *Federal Bureau of Investigation*

The Federal Bureau of Investigation conducted an investigation into individuals laundering over $750,000 of fraudulently obtained funds, including over $390,000 obtained from a fraudulent Paycheck Protection Program loan.

The individuals used a variety of methods to launder funds. Bank Secrecy Act (BSA) data was utilized to identify, locate, and link individuals and their companies to bank fraud; to connect individuals to the criminal network; and to identify facilitating bank accounts and associate previously unknown individuals and companies associated with the fraud ring.

The defendants were charged with conspiracy to commit wire fraud and money laundering.

SAR Review Team – *United States Attorney's Office, Western District of Kentucky*

As part of a multi-agency narcotics and money laundering investigation targeting the subject, federal authorities executing multiple search warrants found and seized narcotics and pill pressing equipment which the subject used to manufacture homemade counterfeit Adderall on his family's property. The subject made his counterfeit pills using methamphetamine and then sold them in bulk to his customers as a vendor on the Dark Web. Authorities also seized drug proceeds, including over $325,000 in cash and bitcoin, valued at over $200,000.

Investigators uncovered the subject's operation through multi-agency collaboration using shipping patterns and Bank Secrecy Act data that indicated money laundering and structuring illuminating information and the trafficking operation well before any narcotics could be tied directly to the subject.

The drug trafficker was sentenced to 132 months in federal prison for charges of possession with intent to distribute methamphetamine, possession of firearms by a prohibited person, and conspiracy to launder drug proceeds.

Review Team – *Federal Bureau of Investigation*

The Federal Bureau of Investigation initiated an investigation into a money laundering case in which the subject first wrote a book on crime and money laundering, then committed crimes. Each month, the subject received approximately $200,000 from an overseas account, withdrew approximately 90 percent of the funds in the form of a cashier's check payable to an individual, and then sent the remainder of the funds to a personal account. All told, the subject laundered approximately $2.5 million.

Financial data was critical to the initiation of this investigation as it provided information related to the movement of illicit funds indicative of money laundering activity. The data also identified specific persons of interest, targets, and subjects, and provided valuable information for investigative leads and intelligence analysis.

The subject pled guilty to two counts of money laundering for using bank accounts to launder over $2 million in proceeds of a bribery and corruption scheme.

SAR Review Team – *Internal Revenue Service-Criminal Investigation*

A SAR review team identified a subject that came to the attention of several financial institutions because of structured currency withdrawals, suspicious deposits, and international wire transfers. Analysis revealed that wire transfer deposits were sent from domestic and international banks and ranged from $2,000 to almost $50,000. Upon receipt of the funds, the subject would withdraw the money and wire transfer the funds to individuals located overseas.

The subject was sentenced to 18 months followed by a three-year term of supervised release. The defendant, originally a victim in a romance scam, later became an important conduit to defraud others.

Significant Fraud – *United States Attorney's Office, Northern District of Indiana*

A public corruption task force's review of financial data identified a pair of individuals illegally using campaign funds for personal expenditures such as gambling, credit card debt, and providing financial support to family members.

One subject pled guilty to wire fraud and the other entered into a deferred prosecution agreement wherein they acknowledged that the Government had sufficient evidence to charge them with wire fraud.

Significant Fraud – *Federal Bureau of Investigation*

The Federal Bureau of Investigation initiated a case involving suspects that conspired with one another and one or more other co-conspirators to defraud a credit union of $94,400. One defendant made multiple visits to the credit union to inquire with numerous banking personnel about negotiating a wire transfer and/or deposit from Nigeria into his banking account. The defendant facilitated the deposit of a fraudulent instrument into the account and later withdrew $22,000 in cash and wired $72,400 to Lagos, Nigeria.

Analysis of financial data was able to affirmatively identify most of the foreign co-conspirators by name, identification, phone number, and/or address, which were subsequently corroborated via subpoenaed records. Two individuals pled guilty to conspiracy to commit bank fraud; a federal judge sentenced them to prison and probation and ordered them to pay restitution.

Significant Fraud – *Federal Bureau of Investigation*

The Federal Bureau of Investigation initiated an investigation into theft at a tribal casino. Analysis revealed that casino supervisors conspired with video technicians to manipulate the electronic gaming machines for their personal benefit. Investigators found that 280 of the 400 computer gaming machines were manipulated. Under the guise of repairing computer gaming machines, the video technicians would manipulate the gaming machines to create false credit vouchers. The video technicians would have their supervisors/co-conspirators approve technical measures to hide evidence of the computer manipulation.

The supervisors used co-conspirators to cash the vouchers and obtain fraudulent proceeds from the resort. The supervisors and co-conspirators would then meet to divide the stolen cash. Each co-conspirator received approximately $800 to $1000 weekly in stolen funds. Investigators estimated the subjects pilfered approximately $5.2 million over a four-year period.

The subjects pled guilty to one count of conspiracy to embezzle more than $1,000 from a tribal gaming establishment and one count of conspiracy to commit computer fraud.

Third Party Money Launderers – *Homeland Security Investigation*

Homeland Security Investigations initiated an investigation into a subject advertising virtual currency exchanges. A phone number associated with the advertisements was reported in financial data. During the course of the investigation, agents purchased $15,000 worth of bitcoin in a peer-to-peer transaction which was later determined to be derived from human trafficking activities.

A separate, unrelated investigation revealed that the kiosks owned by the subject were involved in ransomware payments, romance scams, and other online fraudulent activities.

The money exchange broker pled guilty to federal criminal charges for operating an illegal virtual currency money services business that exchanged up to $25 million – including funds on behalf of criminals – through in-person transactions and a network of cryptocurrency ATM-type kiosks.

Third Party Money Launderers – *Federal Bureau of Investigation*

This Federal Bureau of Investigation case involved multiple individuals using a variety of methods to launder money. Investigators identified over $2.1 million in funds from twelve bank accounts allegedly associated with the fraud scheme as subject to forfeiture. One subject submitted a fraudulent Paycheck Protection Program (PPP) loan application for his business with numerous false and misleading statements.

A financial institution approved and funded a loan of over $395,000, and the defendant disseminated the fraudulently obtained funds to other members of the conspiracy to conceal their true nature. Another subject had previously participated in drug trafficking and financial fraud with two business owners. These business owners agreed to let the defendants use their business bank accounts in return for a percentage of the fraudulent funds deposited in their account. As part of the scheme, several suspects deposited checks totaling $200,000 at a casino. After gambling for less than two hours, they cashed out from the casino and left with approximately $198,750 in cash.

Financial data was utilized extensively to identify, locate, and link individuals and their companies to bank fraud. Seven individuals were charged with laundering over $750,000 of fraudulently obtained funds, including over $390,000 obtained from a fraudulent PPP loan.