INSIDER THREAT INCIDENTS REPORT FOR U.S. GOVERNMENT

From

2020 To 2024

Produced By

National Insider Threat Special Interest Group

Produced For

The Office Of Senator Joni Ernst
Department Of Government Efficiency

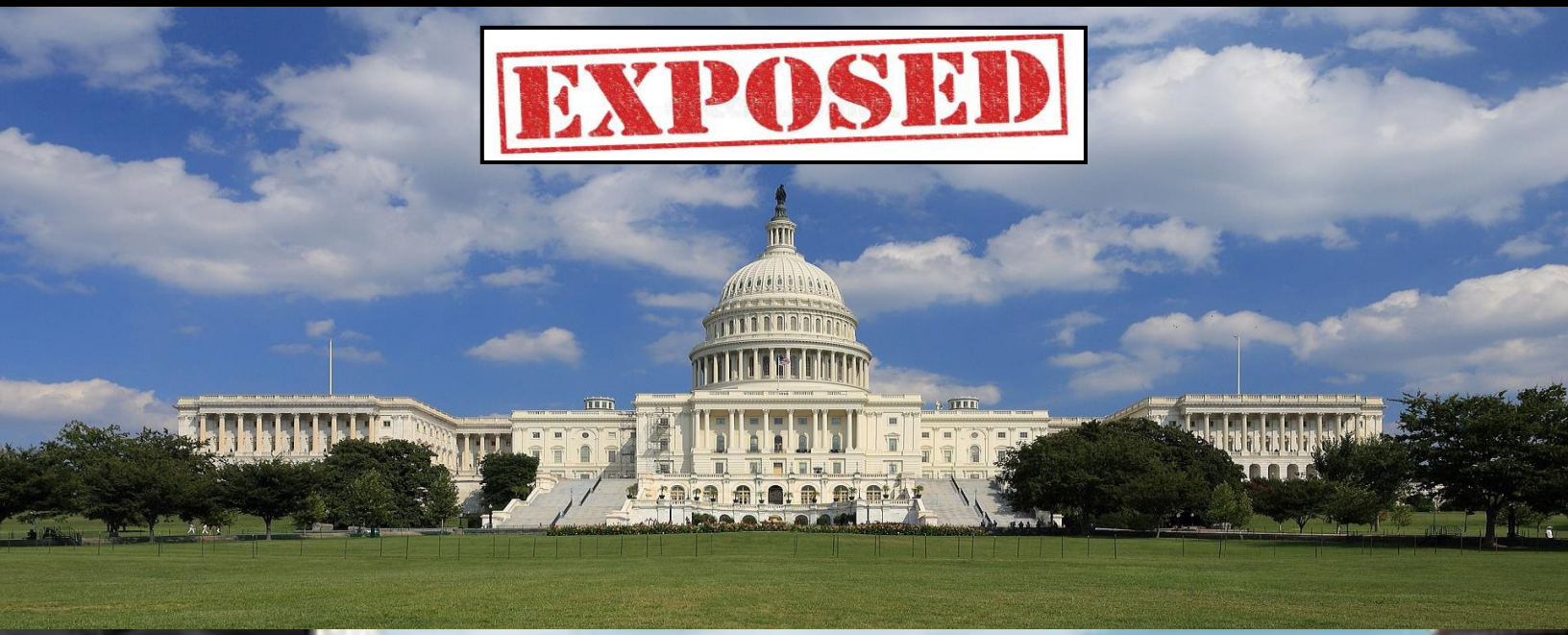

TABLE OF CONTENTS

INSIDER THREATS

A Very Costly And Damaging Problem Within The U.S. Government

OVERVIEW

Senator Ernst's office contacted the National Insider Threat Special Interest Group (NITSIG) in December 2024, and requested a report on Insider Threats in the U.S. Government.

The NITSIG has been conducting extensive research and analyzing the Insider Threat problems occurring in the U.S. and globally for 10+ years. The NITSIG publishes monthly reports on Insider Threat Incidents.

The NITSIG maintains the largest public repositories of Insider Threat incidents covering the U.S. Government and private sector. The monthly and specialized reports like this one provide clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

This report is intended to provide the Department of Government Efficiency (DOGE) with an in-depth look at the magnitude of the Insider Threat problems. How can the U.S. Government be run **1)** Efficiently, **2)** Effectively and **3)** Within Budget, when there are many instances U.S. Government employees and contractors who are taking malicious actions that will impede these 3 objectives?

This report provides a more in depth view of the problems of Fraud, Waste Abuse in the U.S. Government, then a report written by Senator Joni Ernst's Office, titled Out Of Office.

This report will provide deep insights into U.S. Government employees and contractors who intentionally commit theft, fraud, embezzlement, take bribes and also receive kickbacks related to U.S. Government contracting. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live the lifestyles beyond their means.

This report will reveal that many U.S. Government employees and contractors have been sentenced to prison. Others have been arrested, been charged, pleaded guilty or are awaiting further legal action to be taken. The source for the majority of the incidents in this report comes from the Department Of Justice website.

This report covers the time period of 2020 to 2024. While the buildings were empty and the lights were off in many U.S. Government buildings during COVID, theft, embezzlement and fraud were taking place, and continue to occur.

The Insider Threat problem goes beyond President Biden's Administration, and would appear to be an acceptable norm, that has lived in the shadows of the U.S. Government for a long time. For example, the Social Security Administration sent roughly 7,000 federal employees disability benefits in 2008 while they were still taking wages from federal jobs, according to a 2010 Report by the Government Accountability Office.

The U.S. Government is run by money (Taxes) collected from American citizens. But in many cases, U.S. Government employees and contractors are using this money to live lavish lifestyles, pay their debts, fund their gambling addictions or whatever suits them.

How would you like it if your personal bank account had money taken out of your account on a regular basis, to fund the malicious objectives of bank employees? There is really no difference. So regardless of your political affiliation, the information in this report and the initial report written by Senator Ernst's office should raise concerns about how American taxpayers money is being misused.

Oversight and accountability of the U.S. Government's Federal Workforce and the Department of Defense (DoD) starts at the top of the government and is supposed to flow down. But prior to 2025, this appears not to be the case as the information in this report will reveal.

Previously, the U.S. Government has apparently turned their heads and ignored the problems listed in pages 6 to 118 of this report, and did not take a more focused effort to combat theft, fraud and embezzlement by government employees and contractors.

This mentality would not be acceptable in a profit driven corporation. That is why many corporations have Insider Threat Program's (ITP's).

Judging by this report, it appears that U.S. Government Agencies ITP's need to do a much better job of identifying, preventing or mitigating theft, fraud and embezzlement by government employees and contractors.

Every member of the U.S. Congress should read this report, demand accountability and provide answers to American taxpayers on how they intend to do a better job of identifying, preventing and mitigating the many problems described in this report.

Agency heads should also read this report. The incidents listed provide the justification, return on investment and the funding that is needed for developing or enhancing an ITP within an agency. This report also serves as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the agency and understanding Insider Threat Indicators.

The large amount of theft, fraud and embezzlement within the U.S. Post Office, DoD and the Veterans Administration as reflected in this report, can no longer be justified as an acceptable norm.

As many American citizens witnessed in December 2024, there was a big dispute between political parties for passing a continuing resolution spending bill to fund the U.S. Government. In many cases the continuing resolution is providing additional money to government agencies, **but on the back end, taxpayers' money used to fund government agencies was and still is being stolen by U.S. Government employees and contractors at staggering levels.**

Before giving U.S. Government agencies more money, it is very apparent that there needs to be better security controls in place to detect, prevent and mitigate theft, fraud and embezzlement with taxpayers' money.

Some U.S. Government agencies invest hundred of thousands of dollars and into the millions securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem.

There needs to be a much more concentrated effort to establish accountability, provide oversight and promote ethics at the agency head level, and a much greater effort to detect, prevent or mitigate the malicious actions of U.S. Government employees and contractors who steal, embezzle and commit fraud.

The U.S. Government Faces Many Type Of Threats

- Terrorism / Foreign Government Threats
- Border Security Problems
- Economic Espionage From Foreign Governments
- Foreign Government Misinformation / Disinformation Campaigns Against The U.S.
- Network Intrusions From Cyber Attacks - Data Breaches From Hackers / Foreign Governments
- Threats To Critical Infrastructure From Hackers / Foreign Governments
- Illegal Drug Distribution Within The U.S. From Other Countries
- And More….

Examples Of Insider Threats Within The U.S. Government, DoD, Intelligence Community Agencies

- Teleworking Fraud
- COVID Fraud
- Holding Government Job, While Running A Personal Side Business During Working Hours
- Fraudulent Paycheck Increases / Paycheck Padding
- Using Government Funds To Pay For Personal Credit Cards, Mortgage & Vehicle Payments, Gambling, Etc.
- Using Government Funds To Pay Family Members, Significant Others
- Contracting Fraud & Kickback Schemes
- Fraud Schemes Done In Collusion With Family Members And Others
- Bribery Of Government Employee
- Theft Of Government / DoD Assets
- Drug Distribution & Trafficking
- Gun Trafficking
- Espionage
- Theft & Sale Of Personally Identifying Information
- Workplace Harassment & Violence
- Murder

U.S. GOVERNMENT ORGANIZATIONS REFERENCED IN THIS REPORT

The agencies listed below encountered an Insider Threat incident of some type. Publicly available data showed some agencies only having 1 incident, while other agencies had many.

There is also another serious concern that needs to be raised. What is described in this report are incidents where U.S. Government employees and contractors were caught committing theft, fraud, embezzlement, taking bribes or receiving kickbacks. How many incidents went undetected?

- Customs & Border Protection
- Department Of Agriculture
- Department Of Defense
- Department Of Energy
- Department Of Homeland Security
- Department Of Labor
- Department Of Transportation
- Department Of Veterans Affairs
- Drug Enforcement Administration
- Federal Bureau Of Investigation
- Federal Aviation Administration
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Fish & Wildlife
- Forest Service
- General Services Administration
- Internal Revenue Service
- National Aeronautics & Space Administration
- National Guardsman
- National Institutes of Health
- Office Of Personnel Management
- Small Business Administration
- Social Security Administration
- Transportation Security Administration
- U.S. Geological Survey
- U.S. Immigration & Customs Enforcement
- U.S. Marshal Service
- U.S. Postal Service
- U.S. Secret Service
- U.S. State Department Government
- Various Intelligence Community Agencies

U.S. GOVERNMENT
INSIDER THREAT INCIDENTS
FROM 2020 TO 2024

DEPARTMENT OF ENERGY (DOE)

Former Los Alamos National Laboratory Employee Agress To Repay $67,000+ For Unauthorized Time & Expenses Claimed For Business Trips - January 14, 2025

A former employee of Los Alamos National Laboratory has agreed to pay the United States a total of $67,500 to resolve allegations that he violated the False Claims Act by submitting false claims for payment for time allegedly worked and expenses allegedly incurred during business trips.

The settlement resolves allegations that William Wood submitted 23 false claims between July 12, 2016, and December 20, 2017, for trips to various locations in California, including Oakland, Livermore, and Santa Barbara. The United States contends that these claims were for time not actually worked and expenses not actually incurred or without a legitimate business purpose during the period from June 19, 2016, to December 9, 2017.

As part of the settlement, Wood has agreed to pay $67,500, of which $38,549.83 is restitution. In addition to the monetary settlement, Wood has agreed to never seek employment with, or work for, the federal government, its contractors or subcontractors in any capacity funded by or through the federal government, and to never seek a federal government security clearance. (Source)

Department Of Energy Employee Agrees To Pay $96,000+ To Settle False Claims For COVID Economic Injury Disaster Loan For Her Fake Business - June 5, 2024

Lisa Phillips has agreed to pay the United States $96,757.95 to resolve allegations that she violated the federal False Claims Act by submitting false claims to the U.S. Small Business Administration (SBA) to obtain an Economic Injury Disaster Loan (EIDL) and EIDL advance during the height of the COVID-19 pandemic.

On July 10, 2020, Phillips signed and submitted a Loan Authorization and Agreement for an EIDL in the amount of $26,200.00. The United States contends that in her this EIDL application, the defendant made several material misrepresentations including, among other things, that, in 2019, her business had four employees, a gross annual revenue of $150,500, and $90,000 in cost of goods expenses. Phillips also stated that her business opened on January 25, 2017, and that the business was in the Educational Services industry. These misrepresentations were knowingly false; Phillips knew that she did not own or operate a business in the Educational Services industry, that she did not have any employees, and that she had neither the revenue nor cost of goods as stated in the application. In addition to the $26,200 Loan, Phillips received a $4,000 advance. (Source)

Department Of Energy Employee Pleads Guilty To Accepting $18,000 In Bribes In Exchange For Nearly $1 Million In Federal Contracts - June 26, 2023

Some Of The Electronic Components Failed And Caused A Fire Resulting In $1.8 million In damages / Repairs For DOE

Jami Anthony, is the former Small Business Program Liaison and Procurement Officer for a Department of Energy (DOE) laboratory based in Virginia.

She pleaded guilty to receiving bribes as a federal official in connection with a scheme to pay her more than $18,000 in exchange for more than $900,000 in DOE contracts.

Between approximately December 2017 and December 2020, Michael Montenes, the owner of M.S. Hi-Tech, Incorporated (MSHT), a Hauppauge-based distributor of electronic components, paid Anthony approximately $18,800 in bribes to induce her to enter into contracts for electronic components that MSHT supplied to the DOE's Virginia laboratory. Montenes mailed these payments, which ranged from $500 to $7,200, from Long Island to Anthony in Virginia. In exchange for the bribes, Anthony awarded MSHT contracts worth more than $900,000, which represented 95% of all of MSHT's sales to the DOE's Virginia laboratory.

In July 2021, some of the electronic components that Anthony procured from MSHT for DOE based upon Montenes's bribes failed and caused a fire, resulting in approximately $1.8 million in repairs and other costs to DOE. (Source)

Bechtel & AECOM (Department of Energy (DOE) Contractors) Agree To Pay $57.75 Million To Resolve Claims Of Time Charging Fraud at DOE's Hanford Waste Treatment Plant - September 22, 2020

Major Government Contractors Admit to Overcharging between 2009 and 2019 by Billing Time Not Worked

U.S. Federal contractors Bechtel National Inc., Bechtel Corporation (Bechtel), AECOM Energy & Construction, Inc. (AECOM), and their subsidiary Waste Treatment Completion Company, LLC (WTCC), agreed to pay $57,750,000 to the U.S. Department of Justice (DOJ) to resolve claims that Bechtel and AECOM fraudulently overcharged the U.S. Department of Energy (DOE) in connection with its operation of the Hanford Waste Treatment Plant (WTP) project. The False Claims Act (FCA) claims arose from allegations that Bechtel and AECOM management were aware of and failed to prevent inflated labor hours being charged to DOE, and for falsely billing DOE for work not actually performed. (Source)

Department Of Energy Subcontractor Sentenced To Prison For Making $250,000 Of Unauthorized Credit Card Purchases - May 27, 2020

Robert Lazur was employed at BWXT Technical Services Group, Inc., which was working on a subcontract at the Bettis Atomic Power Laboratory in West Mifflin, PA. The contract was funded by Department of Energy.

From approximately January 2016 until December 2017, Lazur used company credit cards and open purchase orders to make hundreds of fraudulent purchases, which were disguised as legitimate contract expenses.
He sold most of the fraudulently obtained items on eBay, so he could convert them to cash. Other items, however, he kept for himself or gave to friends. The total loss was approximately $250,000. (Source)

Department Of Energy Contractor Sentenced To 3 Years Probation For Sabotaging Computer System After Being Terminated / Caused $23,000+ Worth Of Damage - May 20, 2020

Gary Simon resigned from his contracting agency, in about August 2018, he was no longer authorized to access the DOE computer systems.

On October 21, 2018, Simon intentionally accessed the DOE cloud-based system remotely without authorization, using another employees account. He altered and deleted various files. As a result other computer operators were unable to access the computer system. The computer system remained offline for 2-3 hours. Simon's actions resulted in loss to the DOE, in the form of costs associated with responding to the offense, conducting a damage assessment, and restoring data, program, system, and information to its pre-offense condition. (Source)

DEPARTMENT OF COMMERCE (DOC)

Department Of Commerce IT Support Contractor Sentenced To Probation / Home Confinement For Stealing $550,000 Worth Of Government Property And Selling On eBay - January 4, 2023

Dennis Gamarra was employed as a contractor working at the United States Department of Commerce (DOC) within the International Trade Administration (ITA), at an office in Washington, D.C.

Gamarra largely worked to provide information technology (IT) support to the ITA and through his employment had access to certain government-furnished equipment, including Microsoft Surface tablet devices belonging to DOC and issued to DOC employees

Gamarra stole at least one Microsoft Surface Tablet, worth $1,370, removing it from ITA's offices, advertising it for sale online through his eBay account, and ultimately re-selling it to another individual through eBay.

Starting in November 2019, Defendant Gamarra began working as a contractor for the Library of Congress (LOC), at an office in Washington, D.C. While at LOC, providing IT support services. While at LOC, Gamarra removed at least 29 separate Dell laptops from LOC that he knew to belong to LOC, cumulatively worth a total of approximately USD $55,590, advertised them on eBay, and ultimately resold them to different customers through that account. (Source)

DEPARTMENT OF HEALTH & HUMAN SERVICES (HHS)

Department Of Health & Human Services Federal Agent Charge With Drug Trafficking / Witness Tampering - January 8, 2021

Alberico Crespo, a former Special Agent with the Department of Health and Human Services, Office of Inspector General (HHS-OIG), conspired to traffic oxycodone, tamper with witnesses, and obstruct justice and with substantive counts of witness tampering. During the time of the alleged crimes, Crespo worked as part of the South Florida Health Care Fraud Strike Force, made up of interagency teams of federal investigators and prosecutors focused on combating health care fraud and health care-related narcotics trafficking in Southern Florida.

According to the criminal complaint affidavit, the illegal Oxycodone distribution system involved patients, pharmacies, and medical clinics. Patients were recruited and sent to medical clinics to obtain Oxycodone prescriptions that they did not need. Once the patients obtained the prescriptions, they would give them to the recruiter in exchange for money. Recruiters would fill the prescriptions at certain pharmacies and sell the Oxycodone pills (at a mark-up) to third party street dealers.

Crespo used his position as an HHS-OIG Special Agent working on health care fraud cases to protect the Oxycodone operation by monitoring Strike Force investigations involving the operation, accessing and disclosing sensitive law enforcement information to Diaz Gutierrez, a patient recruiter, updating Diaz Gutierrez on the progress of health care fraud investigations, and coaching Diaz Gutierrez on how to lie to investigators and tamper with evidence. (Source)

DEPARTMENT OF INTERIOR (DOI)

Department Of The Interior Employee Sentenced To 5 Years Of Probation For Embezzling $139,000+ Using Fake Vendor Scheme - March 20, 2024

Beginning in May 2018 and continuing through April 2020, George Onwiler embezzled approximately $139,000 from the Bureau of Reclamation (BOR), a component of the United States Department of the Interior. Onwiler was employed as an electrician for the BOR, located in Yuma, Arizona.

In his employment with the BOR, Onwiler was responsible for purchasing commercial and agricultural grade electrical supplies and materials needed for his government work, and he was issued a BOR credit card to make those purchases.

Onwiler embezzled money from the government by using his government issued credit card to pay fictional electrical company suppliers. Onwiler created fake company names and used PayPal and Block/Square to transfer money to himself. Through 47 unauthorized wire transfers, Onwiler transferred $139,168.02 to his personal bank account. These transactions were fraudulent as he did not purchase electrical supplies for the BOR. (Source)

DEPARTMENT OF LABOR (DOL)

Department Of Labor Special Agent Sentenced To Prison For Multiple Fraud Schemes Totaling $197,000+ - August 24, 2023

Former Special Agent with the Department of Labor, Thomas Hartley was sentenced to prison for mail fraud in connection with multiple schemes to commit fraud.

Hartley pleaded guilty and admitted that he obtained a total of $197,366 through multiple fraud schemes. Between April 2020 and September 2021, Hartley applied for and collected Pennsylvania unemployment compensation benefits by claiming that he was unemployed, when in fact Hartley was employed on full time active duty with the New Jersey National Guard. Further, in applying for unemployment benefits, the defendant failed to disclose that he was on military leave from his full-time federal civilian employment with the United States Department of Labor. Hartley thereby utilized the mail to collect approximately $60,284 in unemployment compensation funds to which he was not entitled.

Hartley also fraudulently obtained $23,582 in Basic Allowance for Housing (BAH) funds paid by the Department of the Army, $50,000 in "lost wage" benefits paid by USAA insurance, and $63,500 from his Thrift Savings Plan. (Source)

DEPARTMENT OF TRANSPORTATION (DOT)

Department Of Transportation Border Investigator Pleads Guilty To Extortion / Accepting $2,000 In Bribes From Trucking Company - January 13, 2023

Patrick Gorena was a Border Investigator for Department of Transportation (DOT)'s Federal Motor Carrier Safety Administration.

Gorena admitted that when auditing a trucking company, he did not report safety violations that would have exposed the company to potential fines and the loss of their DOT license. In return, Gorena demanded $3,500.

However, he ultimately accepted $2,000 from an undercover law enforcement officer posing as a representative of the trucking company. (Source)

Department of Transportation Employee Sentenced To Prison For $108,000+ / Enrolled Family Members Into Federal Health Care Plan - October 20, 2020

Edward Stephen was a federal employee with the U.S. Department of Transportation Federal Highway Administration. As a federal employee, he was eligible for health insurance provided by the federal government.

Stephen fraudulently enrolled extended family members into his federal health care plan, knowing they were not eligible for federal health care benefits.

Specifically, Stephen enrolled his sister as though she was his wife and his niece as though she was his step-child so that they would obtain federal health care coverage they were not entitled to receive.

This scheme lasted from 2005 to 2017 and included several years where Stephen resided in and worked in Charleston as a federal employee. When investigators learned of the fraud, Stephen gave a statement to investigators with the Department of Transportation Office of Inspector General. In his statement, Stephen admitting that he fraudulently placed his extended family members on his federal insurance knowing they were not entitled to receive benefits. In total, the Court found that the government was defrauded out of $108,411.59 in fraudulent premium payments and reimbursements. (Source)

FEDERAL AVIATION ADMINISTRATION (FAA)

FAA Contractor Charged For Illegally Acting As An Agent Of The Iranian Government - September 27, 2024

From at least December 2017 through June 2024, Abouzar Rahmati conspired with Iranian government officials and intelligence operatives to act on their behalf in the United States, including by meeting with Iranian intelligence officers in Iran, communicating with coconspirators using a cover story to hide his conduct, obtaining employment with an FAA contractor with access to sensitive non-public information, and obtaining open-source and non-public materials about the U.S. solar energy industry and providing it to Iranian intelligence.

From June 2009 to May 2010, Rahmati served as a First Lieutenant in the Islamic Revolutionary Guard Corps (IRGC), an Iranian military and counterintelligence organization under the authority of the Supreme Leader of Iran. After being discharged from the IRGC, Rahmati lied to the United States government regarding his military service with the IRGC in order to, among other things, gain employment as a U.S. government contractor. (Source)

Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System / Shutdown Airport For 2 Weeks- September 26, 2014

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared ATC Zero after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

Over the course of 17 days, FAA technical teams worked 24 hours a day alongside the Harris Corporation to completely rebuild and replace the destroyed communications equipment. They restored, installed and tested more than 20 racks of equipment, 835 telecommunications circuits and more than 10 miles of cables.

The 2015 FAA repot concluded that the contingency plans and security protocols were insufficient at the Chicago Airport when this incident happened in 2014. (Source)

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

Federal Deposit Insurance Corporation Workplace Filled With Sexual Harassment According To Independent Probe - May 7, 2024

The Federal Deposit Insurance Corporation (FDIC) is a workplace rife with sexual harassment and discrimination, an independent investigation recently alleged.

The investigation was commissioned by the FDIC last year after revelations of widespread misconduct came to light via a Wall Street Journal report.

Law firm Cleary Gottlieb spoke with 500 FDIC employees, out of close to 6,000 total, many who recounted experiences of sexual harassment and described widespread fear of retaliation.

Martin J. Gruenberg is the acting Chairman of the FDIC.

According to the report Gruenberg isn't the "root cause of all the workplace issues," the authors note, but "'tone at the top' is important."

Gruenberg also has a reputation for being harsh, demeaning and insulting, they report, which "raises questions about the credibility of the leadership's response to the crisis and the 'moral authority' to lead a cultural transformation." Some lawmakers are already calling for Gruenberg's resignation, including at least one Democrat.

The highly detailed 234 age report is filled with explosive details. "A woman examiner reported on the shock of receiving a picture of an FDIC senior examiner's private parts out of the blue while serving on detail in a field office, only to be told later by others in that field office that she should stay away from him because he had a 'reputation,'" authors of the report wrote.

"A number of employees recounted homophobic statements made by their Field Office Supervisor, including referring to gay men as 'little girls,' resulting in one of them, at least, believing he had to hide that he was gay."

What did Gruenberg, the acting Chairman of the FDIC have to say: "To anyone who experienced sexual harassment or other misconduct at the FDIC, I again want to express how very sorry I am," he wrote to staff ahead of the report's release, per the WSJ. "I also want to apologize for any shortcomings on my part." (Source)

GENERAL SERVICES ADMINISTRATION (GSA)

GSA Construction Control Representative Official Sentenced To Prison For Accepting $400,000+ In Bribes - March 2, 2023

Charles Jones was employed as a Supervisory Construction Control Representative with the GSA in Richmond. He had responsibility for the management and oversight of construction and renovation projects at certain federal buildings throughout the Norfolk, Richmond, and Alexandria areas.

Beginning in approximately December of 2015 and continuing through August 2019, Jones received bribes totaling $411,192 from Daniel Crowe, in exchange for awarding them federal construction projects to his companies. In October of 2019, Jones received a cash payment from Jennifer Strickland, the President of SDC Contracting LLC, in exchange for awarding a contract valued at approximately $1,369,501. (Source)

GSA Employee Sentenced To Prison For Accepting $12,000+ Of Bribes For 6 Years To Help Company Maintain Contract With GSA - October 5, 2020

Ronnie Simpkins was employed by the General Services Administration (GSA) as a Contract Specialist, informally known as a Contracting Officer, in procurement related positions.

Simpkins admitted that for approximately six years between 2011 and 2017, he accepted cash, meals, and furniture from two company officials, to use his position to help these company official maintain its GSA Schedule contract.

He admitted to meeting the company officials over a dozen times at various restaurants in Northern Virginia, the company officials' residences, and other places, often outside of normal GSA business hours and on weekends. At these meetings, the company officials treated Simpkins to meals and gave him cash totaling thousands of dollars into the teens. In July 2016, Simpkins accepted more than $2,000 worth of furniture paid for by the officials. Simpkins admitted to taking more than $12,000 in cash and furniture from the company officials. (Source)

INTERNAL REVENUE SERVICE (IRS)

5 IRS Employees Sentenced To Prison For $1 Million+ COVID-19 Relief Fraud Scheme / Used Funds To Purchase Cars, Travel, Etc. - September 30, 2024

Brian Saulsberry was employed by the IRS as a Program Evaluation and Risk Analyst in the Human Capital Office in Memphis, Tennessee. Saulsberry laundered funds he received from a scheme to defraud the Economic Injury Disaster Loan (EIDL) program, a federal stimulus program authorized to provide loans to small businesses experiencing substantial financial disruptions due to the COVID-19 pandemic as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Saulsberry submitted false EIDL applications and obtained $171,400 in loan funds. After obtaining the fraudulent loan funds, Saulsberry transferred the funds to his personal checking account. He then used the loan funds for purposes not authorized by the EIDL Program, but instead transferred $100,000 to an investment account, knowing that the property involved in the transaction was derived from unlawful activity.

In addition to Saulsberry, four other former IRS employees, Courtney Westmoreland, Fatina Hewitt, Roderick White and Tina Humes were convicted for defrauding federal stimulus programs authorized as part of the CARES Act, including the EIDL Program and the Paycheck Protection Program.

The five former federal employees collectively sought over $1 million. They then used the loan funds to invest in personal accounts, purchase cars and luxury goods, and pay for personal travel, including trips to Las Vegas. (Source)

IRS Information Technology Supervisor Pleads Guilty To Accepting $120,000+ In Bribes From Government Subcontractor Whom He Attempted to Extort - September 11, 2024

Satbir Thukral worked for the IRS as a computer engineer and supervised various information technology contracts.

In September 2018, Company 1 began working on a subcontract for the IRS that Thukral supervised. Starting in October 2018, Thukral sought cash payments from Company 1's owner, Individual 1, constituting a portion of the earnings from Company 1's work on the IRS subcontract. Between 2018 and 2020, Individual 1 made multiple cash payments to Thukral totaling more than $120,000.

In February 2021, when Individual 1 told Thukral that Individual 1 would not pay any more money, Thukral attempted to extort Individual 1 by threatening that Individual 1 would suffer economic consequences if the payments did not continue. In early February 2023, Individual 1 recorded an in-person meeting with Thukral at the direction of law enforcement. During the meeting, Individual 1 told Thukral that the FBI had asked about bank withdrawals that Individual 1 had made to pay Thukral, and Thukral instructed Individual 1 to lie to the FBI about the nature of the cash withdrawals. Later that same day, to assist and induce Individual 1 to lie to the FBI and to further the concealment of the payments, Thukral returned a portion of the proceeds that Thukral had received from Individual 1.

In a separate scheme, in July 2022, Thukral received approximately $2,800 in cash from a manager at a prime contractor with the IRS. The manager made the payment, in part, in return for Thukral's facilitating the continued employment of two underqualified individuals at two other IRS subcontractors with whom the manager had an affiliation. In addition, at the time of the payment, the manager believed that Thukral, who had been selected to serve on a three-person panel that would have evaluated the technical feasibility of bids of an upcoming IRS contract valued at approximately $200 million, could influence the valuations to the manager's benefit. (Source)

IRS Contractor Sentenced To Prison For Disclosing The Tax Returns Of President Trump To News Organizations - January 29, 2024

Charles Littlejohn while working at the IRS as a government contractor, stole tax return information associated with a high-ranking government official (Donald Trump - Public Official A). Littlejohn accessed tax returns associated with Public Official A (And Related Individuals &d Entities) on an IRS database after using broad search parameters designed to conceal the true purpose of his queries. He then uploaded the tax returns to a private website in order to avoid IRS protocols established to detect and prevent large downloads or uploads from IRS devices or systems.

Littlejohn then saved the tax returns to multiple personal storage devices, including an iPod, before contacting News Organization 1. Between around August 2019 and October 2019, Littlejohn provided News Organization 1 with the tax return information associated with Public Official A. Littlejohn subsequently stole additional tax return information related to Public Official A and provided it to News Organization 1. Beginning in September 2020, News Organization 1 published a series of articles about Public Official A's tax returns using the tax return information obtained from Littlejohn. (Source)

IRS Agent And 5 Five Other Individuals Charged In $3 Million COVID-Fraud Scheme - May 10, 2023

The U.S. Attorney's Office has is charging six defendants with a variety of crimes in connection with an alleged scheme to obtain millions of dollars by submitting fraudulent loan applications through the U.S. government's Payroll Protection Program (PPP).

Central to the allegations in the charging documents is the role of Frank Mosley a former IRS Revenue Agent and current City of Oakland Tax Enforcement Officer. Mosley conspired with others to submit fraudulent PPP-loan applications and then, after securing the proceeds from the loans, used his share of the illegally-obtained proceeds for personal investments and expenses. The defendants, including Mosely, received approximately $3 million as a result of submitting fraudulent loan applications under the PPP program. (Source)

IRS Employee Sentenced To Prison for Scheme To Defraud IRS Of $190,000 And Commit Identity Theft - May 8, 2023

Deena Lan was sentenced today to four years and six months in prison and ordered to pay $191,597 in restitution following her convictions for preparing and filing false tax returns for other individuals, underreporting her own taxable income on her personal tax returns, and committing wire fraud and aggravated identity theft.

From 2012 through 2016, Lee, in her role as a tax preparer, put materially false information on customers' tax returns without their knowledge or consent and submitted the returns to the IRS. As part of the scheme, Lee obtained the identification of multiple individuals and falsely listed these individuals as child care providers on multiple customers' tax returns without their knowledge or consent. (Source)

IRS Employee Pleads Guilty To Fraudulently Obtaining $62,000+ In CARES Act Funds While Working For IRS - September 28, 2022

In July 2020, Charles Clark fraudulently applied for a loan under the Economic Injury Disaster Loan (EIDL) program.

In his EIDL application, Clark falsely claimed to have been an independent contractor working in the "Hair & Nail Salon" industry when he was working as a full-time IRS employee. He obtained $62,300 in funds which he then misused by spending them on renovating an investment property he owned. (Source)

Federal Jury Convicts IRS IT Specialist Of $58,000+ Of Fraud For Personal Benefit - July 19, 2021

A former Information Technology Specialist for the IRS, Kwashie Zilevu operated a fraud scheme in which he used a line of credit in a victim's name to make hundreds of purchases totaling more than $58,000, for his own benefit. In connection with this scheme, identity information was obtained from the Dark Web. Ultimately, a credit card in the victim's name was mailed to the defendant's home in Woodbridge.

Zilevu's purchases included international plane tickets, expensive hotel rooms, interior decorating services, and construction materials used to remodel his home, among other goods and services. Evidence presented at trial also demonstrated that Zilevu made fraudulent payments to himself using financial instruments belonging to other people, including routing charitable donations to a fictitious African charity website he created, controlled, and used to further his criminal activity, and by receiving payments from a PayPal account associated with the credit card opened in the victim's name. (Source)

IRS Employee Sentenced To Prison For Stealing $5,200+ Of Tax Refunds - September 29, 2020

Tamara Miller was employed by the IRS as a data transcriber at the Kansas City Service Center. As part of her duties, Miller handled individual income tax returns received by mail at the Kansas City Service Center.

Miller selected tax returns on which the "Refund" section did not show a routing number or account number for a direct deposit to a financial institution (indicating the taxpayer elected to have the refund paid by a U.S. Treasury check). Miller used taxpayers' means of identification, including names and Social Security numbers, shown on their tax returns to apply for accounts at online banks that issued prepaid debit cards. If Miller succeeded in opening an online account with a taxpayer's means of identification, she entered the routing number and account number for the fraudulently created account in the "Refund" section of the taxpayer's Form 1040. Miller had access to the fraudulently created account; the taxpayer did not know the account existed.

As an alternative means of fraudulently altering taxpayers' returns, Miller entered the routing and account numbers for an existing online account to which she had access in the "Refund" section of the Forms 1040, thereby falsely representing that the taxpayer elected to have the refund amount deposited directly to that account. (Source)

NASA

NASA - JPL Employee Pleads Guilty To COVID-19 Economic Relief Program Fraud ($151,000) / Used Some Proceeds To Grow Marijuana - July 24, 2023

A NASA Jet Propulsion Laboratory (JPL) employee has agreed to plead guilty to defrauding a government-sponsored loan program designed to help people and businesses survive the COVID-19 pandemic's economic impact and has admitted that he used part of the proceeds to fund illegal marijuana cultivation, the Justice Department announced today.

Armen Hovanesian was a Cost Control And Budget Planning Resource Analyst for the NASA Jet Propulsion Laboratory (JPL).

From June 2020 to October 2020, Hovanesian submitted three loan applications in the names of business entities under his control to the Economic Injury Disaster Loan Program (EIDL), a program administered by the Small Business Administration (SBA) that provided low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters, including businesses impacted by the COVID-19 pandemic.

Hovanesian admitted to making false and fraudulent statements in the loan applications concerning the gross revenues each of the businesses had generated in the preceding year as well as false and fraudulent statements concerning his intended use of loan proceeds.

Hovanesian certified to the SBA under penalty of perjury that he would "use all the proceeds" of the loans for which he applied and caused others to apply for "solely as working capital to alleviate economic injury caused by disaster" consistent with the terms and limitations of the EIDL program. But Hovanesian instead applied those proceeds toward his own prohibited personal benefit to repay a personal real-estate debt and fund his illegal marijuana cultivation. Hovanesian fraudulently caused the SBA to transfer via interstate wire EIDL proceeds totaling $151,900. (Source)

NASA Contractor Charged With Smuggling And Exporting American Aviation Technology To Beijing University - May 26, 2022

Jonathan Yet Wing Soong is charged with smuggling and violating export control laws by allegedly secretly funneling sensitive aeronautics software to a Beijing university.

Soong was employed by Universities Space Research Association (USRA) between April 2016 and September 2020 as a program administrator. USRA is a nonprofit corporation contracted by the National Aeronautics and Space Administration (NASA) to distribute domestically and internationally sensitive aeronautics-related software developed through the Army's Software Transfer Agreement (STA) program. As USRA's STA program administrator, Soong was responsible for overseeing certain software license sales, conducting export compliance screening of customers, generating software licenses, and, on occasion, physically exporting software.

Soong unlawfully and without a license exported and facilitated the sale and transfer of software to Beihang University. (Source)

NASA Senior Executive Sentenced To Prison For $272,000 Of COVID Loan Fraud / Used Funds To Pay Credit Card Bills, Buy French Bulldog, Swimming Pool, Etc. - July 17, 2021

Andrew Tezna says he regretted applying for coronavirus pandemic relief loans from the Small Business Administration almost as soon as he filed the paperwork. The NASA senior executive tried, unsuccessfully, to cancel one of the applications.

But when the $272,000 arrived, Tezna admitted, he used the cash as he had planned — to pay down his massive debts while incurring new costs, including $6,450 for a French bulldog and nearly $50,000 for a swimming pool. But under the surface, Tezna was living a different kind of archetypal American tale. To keep up his family's lifestyle, he went deep into debt.

Tezna used the funds to pay off over $140,000 on credit cards and $18,000 on a car loan, among other debts, while buying new cars and renewing a Disney timeshare.

He confessed to applying for three loans through the PPP — one for his wife's design business, which in reality had no employees and little income, and two for companies he invented using his and his mother-in-law's names.

Tezna also collected unemployment benefits fraudulently in his mother-in-law's name, he admitted, and applied unsuccessfully for more small-business loans through his wife's company. He did not report $36,000 in rent from a friend who lived with him and his wife, according to court records.

Tezna who helped oversee NASA spending, was sentenced to 18 months in prison. Tezna lost his job overseeing policy for NASA's Chief Financial Officer and has been blocked from any future government-related work. Tezna is now working as a loader at Lowe's, earning $14 an hour. (Source)

NATIONAL INSTITUTES OF HEALTH (NIH)

NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers - April 22, 2021

More than 500 federally funded scientists are under investigation for being compromised by China and other foreign powers, the National Institutes of Health revealed.

The federal health officials told a Senate committee that they are fighting to keep up with large-scale Chinese efforts to corrupt American researchers and steal intellectual property that scientists hope will lead to biomedical advances.

NIH has contacted more than 90 institutions about more than 200 scientists they're concerned about, said Dr. Lauer, NIH deputy director for extramural research. But the investigations' workload is weighing down the nation's top medical research agency, and new cases are turning up constantly across the government.

China has targeted research throughout the economy from corn growers to cancer researchers. Last year, Dr. Lauer said, more than 90% of the scientists under investigation had received support from China.

U.S. officials also have sounded the alarm that China has tried to hack COVID-19 research and is intent on pilfering U.S. science and technology because it believes American innovation will enable it to overtake the U.S. as a global superpower.

One way China and other hostile adversaries target American innovation is through government-sponsored talent recruitment programs that the U.S. government has said can involve theft of trade secrets, breaking export control laws and violating conflict of interest policies. (Source)

OFFICE OF PERSONNEL MANAGMENT (OPM)

OPM Federal Investigator Sentenced To Prison For Fabricating 22 False Reports For Background Checks Interviews He Never Conducted - June 20, 2024

Christopher Laughlin began working at the United States Office of Personnel Management as a federal background investigator in May of 2018. His position was transferred to the Defense Counterintelligence and Security Agency (DCSA) on September 30, 2019.

On August 2, 2021, as part of DCSA's internal control process, an individual reported that Laughlin never interviewed them, contrary to Laughlin's statements in an investigation report. DCSA investigated and identified three other sources Laughlin claimed to have interviewed in the same investigation who all stated they'd never been interviewed. DCSA's Office of the Inspector General then initiated a formal investigation into Laughlin's conduct.

Investigators determined that between February 18 and September 1, 2021, Laughlin submitted at least 22 false reports containing fabricated statements from at least 43 interviews that never actually happened. The reports included statements that the sources purportedly made to Laughlin by people he never spoke with.

DCSA spent $69.846.214 in payroll and travel to conduct the investigations that Laughlin fabricated. (Source)

SMALL BUSINESS ADMINISTRATION (SBA)

SBA Administration Employee Convicted For Accepting Bribes To Process $800,000+ Of Loan Applications - September 25, 2024

Angela Chew conspired with three others to submit applications for COVID-19 Economic Injury Disaster Loans (EIDLs) containing false and fraudulent information in exchange for bribe payments.

Chew used her position as a loan specialist for the Small Business Administration (SBA) to internally access those loan applications that she and a co-conspirator had submitted on behalf of others. Chew then took actions on the applications within the SBA's internal processing system that moved the loans towards approval. For example, Chew submitted a loan on behalf of a co-conspirator's business that she knew was not active or operating at the time she submitted the loan. The loan was flagged as a duplicate by the SBA's internal system, which stopped the application from progressing toward approval and funding. Chew then entered the SBA's loan processing system, accessed the loan application, reactivated it, and manipulated the loan's status multiple times in order to progress the application toward approval and funding in the amount of $150,000. In exchange, Chew received thousands of dollars in bribe payments from two of her co-conspirators. The evidence showed that Chew caused the funding of at least six EIDL applications, for a total loss of over $800,000. (Source)

SBA Administration Employee Sentenced To Prison For Role In $11 Million COVID Relief Fraud Scheme - May 25, 2023

Lakeith Faulkner was an employee of the Small Business Administration (SBA). He used his position to assist borrowers in submitting over $11 Million worth of fraudulent loan applications for Economic Injury Disaster Loans, which were intended to help small businesses recover from the economic impacts of the COVID-19 pandemic. In return for his assistance in submitting the fraudulent loan applications, those borrowers paid Faulkner and his co-defendant, Norman Beckwood, $2.3 Million. (Source)

SBA Employee Sentenced To Prison For Role In $18,000+ Identity Theft Scheme - April 19, 2022

Jay Soulliere was a Disaster Recovery Specialist for the Small Business Administration (SBA) from September 2020 until March 2021. His job responsibilities included assisting people applying for disaster-related loans.

In the fall of 2020, Soulliere stole from SBA's computer system the personal information of two victims who had applied for loans. Soulliere gave that information to a co-conspirator, Matthew Moore Vodak, Jr., who used it to commit various acts of identity theft, including buying a Land Rover with a fraudulent check and driver's license, taking over a credit card, applying for loans and credit, and producing fake identification documents. Soulliere also listed one of the victims as a member of his household in a bid to obtain state benefits. During the offense and the prosecution, Soulliere repeatedly used methamphetamine and he absconded from a halfway house. When he was arrested by federal agents, he had another person's identification document in his possession and lied to agents about his identity.

Soulliere pled guilty to conspiracy to commit identity theft and aggravated identity theft. Soulliere was also sentenced to three years of supervised release following incarceration and ordered to pay more than $18,000 in restitution. (Source)

SBA Administration Employee Sentenced To Prison For Defrauding Hurricane Victims Of $285,000 / Used Funds For Personal Use - August 31, 2021

Keonna Davis was a disaster recovery specialist for the U.S. Small Business Administration. She pleaded guilty to wire fraud and aggravated identity theft.

Davis took personal information from people applying for disaster relief loans after Hurricane Harvey, obtained the loans and drew money from the applicants' accounts and used it to lease a $4,900 French bulldog and make other purchases totaling $285,430. (Source)

SOCIAL SECURITY ADMINISTRATION (SSA)

SSA Employee Sentenced To Prison For $49,000+ Fraudulent Telework Scheme While Working Another Job - September 26, 2024

Christopher Markham was employed by the Social Security Administration and assigned to an office in Anderson, Indiana.

Between February 13, 2019, and June 17, 2022, Markham engaged in a scheme by which he made it appear as though he was teleworking full-time for Social Security Administration (SSA) during workdays, when in reality he was earning income working as a home inspector for his personal business. Markham was paid his full federal salary and benefits, while concealing the fact that he was working for his personal business and not for SSA.

Markham routinely performed home inspections for his personal business during the workweek while purporting to "telework" on official SSA time. He concealed the fact that he was not performing SSA work during official work hours by having his wife and his mother access the SSA computer system and send emails to supervisors to make it appear as though he was online and working.

Markham nevertheless sought to be paid in full during this period and submitted 53 fraudulent time reports to SSA's online timekeeping portal, as well as falsified daily work logs to his supervisors.

Additionally, Markham engaged in other fraud schemes to obtain Emergency Paid Leave by falsely claiming he was required to stay home to take care of his children. In fact, his children were in daycare, and he was again performing work for and earning income from his personal business. He allegedly performed at least 70 home inspections for his personal business while claiming to be providing emergency care for his children.

Finally, on multiple occasions, Markham fraudulently claimed benefits under the Family and Medical Leave Act "FMLA) by falsely claiming he was unable to work due to illness—when he was actually doing home inspections for his personal business. Markham even attended an F.C. Tucker retreat promoting his business while claiming he was on FMLA leave.

On June 4 and 5, 2020, Markham was granted administrative leave after claiming that the internet wire to his home had been cut. Markham advised that his internet provider would not be able to send anyone to his home to repair the wire until Friday, June 5, 2020. In reality, his internet provider had no record of a damaged wire, and Markham used the administrative leave to take an unapproved, paid vacation to Gatlinburg, Tennessee.

In total, Markham's fraudulent conduct caused a loss to the SSA of approximately $49,255, which he has been court ordered to repay. Markham's failure to perform his duties caused needy members of the public to have their social security benefits delayed, including people with autism, blindness, and end stage cancer. (Source)

SSA Claims Specialist Sentenced To Prison For $288,000+ COVID Pandemic Unemployment Assistance Fraud Scheme / Used Funds For Personal Expenses - April 3, 2024

Takiyah Austin pleaded guilty to one count wire fraud and one count of aggravated identify theft.

From May 2020 to May 2021, Austin, a Claims Specialist with the Social Security Administration (SSA), filed Pandemic Unemployment Assistance claims for ineligible recipients in exchange for payment from the individuals. Austin filed claims after accessing SSA databases to obtain the personal identifying information from unsuspecting individuals and then diverted the unemployment funds to addresses she controlled in order to use the funds for her own personal expenses. Through the scheme, Austin defrauded the government of over $288,000. (Source)

SSA Claims Specialist Employee Charged For Embezzling $1.8 Million+ Of Social Security Funds For 12 Years - March 14, 2024

Myrna Faria was employed by the Social Security Administration (SSA) from approximately 1991 through 2019 as a Social Insurance Specialist and Claims Specialist" working in the Workload Support Unit in San Juan, Puerto Rico.

From March 2012 through March 2024, Faria embezzled and stole SSA funds, namely Retirement Insurance Benefits, Survivors Insurance Benefits and Auxiliary Benefit payments, to which she knew she was not entitled. In total, Faria stole approximately $1,812,455.10.

Faria utilized her position within SSA to submit false claims on behalf of others, using the identity of individuals she believed to be deceased. She then approved those false claims and submitted her own bank and address information to fraudulently receive the corresponding SSA beneficiary proceeds. Faria proceeded to withdraw, transfer, and spend the money from the accounts that fraudulently obtained the SSA funds. Over the span of twelve years, Faria submitted and approved 13 fraudulent claims. A total of 10 fraudulent claims were still active and receiving funds as of the date of the Indictment. (Source)

SSA Claims Specialist Sentenced To Prison For Stealing $324,000+ By Creating 10 Fictitious Children - July 13, 2023

Beginning around August 2019 and continuing through September 2021, Justin Skiff used his position as a Claims Specialist with the Social Security Administration (SSA) to fraudulently obtain money from the SSA.

Skiff used his knowledge and access to establish Social Security Numbers for ten fictitious children. He then established fictitious records of entitlements for surviving child benefits which he connected to the record of a real deceased individual. These benefits were deposited into a bank account accessible to Skiff through debit cards he directed to be mailed to a P.O. Box to which he had access. Skiff withdrew money and made purchases from this account from October 2019 through September 2021 for a total amount of $324,201.44. (Source)

SSA Operations Supervisor Sentenced To Prison For $760,000 Wire Fraud / Identity Theft Scheme - October 4, 2021

Stephanie Chavis was an Operations Supervisor at the Social Security Administration (SSA).

Chavis had access to SSA beneficiary accounts and associated personal identifying information (PII). Between approximately August 2010 and April 2018, Chavis caused over $760,000 in SSI benefits to be electronically deposited into nine different bank accounts held in her name, and in the names of various family members, by making false and fraudulent representations to fellow SSA employees, including claims representatives and other supervisors. The investigation established that Chavis used her government-issued PIN number to query the accounts of approximately 62 program beneficiaries and used their PII to generate the fraudulent payment requests. The beneficiaries targeted by Chavis included incarcerated individuals who were not entitled to payments, individuals who had been suspended or terminated from the SSI program, and beneficiaries who were legitimately owed SSI funds.

To circumvent SSA policy requirements, Chavis provided the beneficiary PII and account information for deposit purposes to unsuspecting claims representatives and asked them to create approximately 100 fraudulent payment requests. After the requests were created, Chavis either approved them herself or asked other SSA employees to process the approvals. Thereafter, the stolen funds were deposited into the bank accounts under Chavis's control. (Source)

SSA Employee Pleads Guilty To Theft Of $100,000+ / Identity Theft For Personal Use (Jewelry, Airline Tickets, Gambling) - November 18, 2021

Sean Okrzesik admitted that from February 2020 through February 2021, he opened bank accounts using the names and Social Security numbers of various Supplemental Security Income (SSI) beneficiaries or their representative payees.

Okrzesik also admitted that once these accounts had been created, he would divert SSI benefit payments intended for these beneficiaries into the accounts, which he then used to pay personal expenses including the purchase of video gaming equipment, a custom suit, jewelry, airline tickets to the Caribbean, and online gambling. The total amount of SSI benefits stolen by Okrzesik was $103,798.77. (Source)

SSA Claims Specialist Pleads Guilty To Charges For Scheme To Obtain $236,000+ in Social Security Benefits By Allegedly Submitting Fictitious Claims - January 15, 2021

Cheikh Cisse was employed by the Social Security Administration (SSA) as a Claims Specialist in SSA's Office of International Operations. Cisse admitted that between July 2018 and March 2019, he filed fictitious claims for benefits using stolen identities and identity documents he obtained through the course of his employment with SSA in order to steal or attempt to steal over $236,000 from SSA.

Cisse was responsible for reviewing the identity documents of social security claimants living abroad, such as passports, marriage certificates, and identity cards. Cisse then created new, fictitious identities in SSA's database, often using information from the foreign identity documents he reviewed, which were issued social security numbers (SSNs). Cisse used the fictitious identities to file fraudulent claims for social security divorced spouse survivor's benefits against actual deceased individuals, directing the benefits payments to debit cards or bank accounts he opened in the names of the fictitious identities using the identity documents he obtained through his employment. (Source)

SSA Claims Specialist Sentenced To Prison For Misappropriating $732,000 In Fraudulent Benefits For Personal Use - October 2, 2020

Anne Aroste worked as a claims specialist at the SSA's field office. Aroste was responsible for processing applications for Social Security benefits via the agency's electronic records system. From 2013 to 2018, Aroste used the Social Security earnings records of deceased workers to create fraudulent applications for benefits. She then used her employee credentials to approve the applications and route the payments to bank accounts she controlled.

Aroste used the fraud proceeds to make credit card payments, mortgage payments, and car loan payments, including payments for a 2015 Mercedes-Benz sport-utility vehicle. She also used fraud proceeds to purchase clothing, groceries, jewelry, and cosmetics. (Source)

SSA Claims Specialist Sentenced To Prison For Stealing $70,000+ From Social Security Beneficiaries - March 6, 2020

From 2017 - 2018, Kianna Parrot worked as a claims specialist for the Social Security Administration, She used her government computer to defraud beneficiaries out of their Supplemental Security Insurance payments.

Officials with the Social Security Administration first noticed suspicious deposits to Parrot's personal accounts from SSI accounts. The ensuing investigation revealed that Parrot diverted SSI underpayments intended for legitimate beneficiaries to her own account. She accomplished this theft by using her Social Security Administration computer and personal identifying number to access the social security records of individuals owed SSI underpayments. Once she accessed these records, she would initiate a payment transaction which listed the names and social security numbers of the true beneficiaries, but which listed Parrot's banking information. Parrot ultimately stole more than $70,000. (Source)

U.S. DEPARTMENT OF AGRICULTURE (USDA)

Department Of Agriculture Employee Sentenced To Prison For Role In $1 Million Contracting Fraud Scheme To Benefit His Private Company - October 25, 2024

Ifediora Oli, an employee of the United States Department of Agriculture (USDA), was sentenced to prison for conspiring with two local government officials to defraud the District of Columbia and the Washington Metropolitan Area Transit Authority (WMATA) of money, property, and their employees' honest services. As a result of the conspiracy, a private company owned and operated by Oli improperly received over $1 million. Between 2018 and 2023 Oli was employed at USDA while separately acting as the Principal of Highbury Global Group, Inc. (Highbury).

Obinna Ogbu was employed at WMATA as an information technology (IT) customer support manager who sometimes also served as a WMATA contracting officer's technical representative (COTR) on certain WMATA contracts. Bridgette Crowell was a public employee who managed contracts at the District's Office of Contracting and Procurement (OCP) and, before that, WMATA.

Beginning in 2018, Oli and Ogbu agreed to use Ogbu's official position and connection to Crowell to steer funds from WMATA IT-related contracts to Highbury. As part of the conspiracy, Oli and Ogbu agreed to commit bribery. Specifically, Oli and Ogbu agreed that Oli would give Ogbu things of value in exchange for Ogbu misusing his position at WMATA to benefit Oli. By 2023, Oli and Highbury had received nearly $500,000 through this corrupt scheme. (Source)

Department Of Agriculture Program Director & Nephew Arrested For $400,000 Fake Contract / Kickback Scheme - May 22, 2024

From August 2015 through November 2022, Kirk Perry, a United States Department of Agriculture (USDA) Program Director, arranged for Jamarea Grant (Perry's Nephew) to be hired by two companies under contract with the USDA Office for Civil Rights.

Grant reported directly to Perry, and the two of them conspired to bill the government for work that Grant did not actually perform. Grant is alleged to have received nearly $400,000 for work he did not do, and, in return, kicked back approximately $125,000 to Perry as part of the criminal scheme. (Source)

Department Of Agriculture Employee Accepted Bribe Payment From Contractors - August 24, 2023

Roberto Rodriguez worked or the U.S. Department Of Agriculture (USDA) as a Rural Development Loan Specialist.

From on or about January 2021 and continuing through Aug. 22, Rodriguez accepted bribe payments from Sandoval and Diaz. In return, Rodriguez allegedly referred applicants of the USDA 504 Single Family Housing Repair Grant and Loan program to the contractors.

Rodriguez did knowingly, corruptly and in violation of his official duty, accepted payments from Sandoval and Diaz, according to the allegations. The contractors allegedly paid the bribes with the intent to influence official acts after the federally-funded repairs were completed. (Source)

Department Of Agriculture Animal Inspector Sentenced To Prison For Accepting $40,000+ In Bribes To Allow Cattle To Enter U.S. Without Proper Quarantine Or Inspection - June 1, 2023

Roberto Adams was an employed at the U.S. Department of Agriculture (USDA) as a lead animal health technician for 10 years. In that role, he was responsible for inspecting and quarantining or excluding tick-infested or diseased cattle. He was only one of two technicians the USDA employed in Laredo and exercised high level decision-making authority.

Adams admitted he accepted over $40,000 in bribe payments from Mexican cattle brokers while acting in his official position as a USDA employee. In return, he allowed cattle to enter the United States without proper quarantine or inspection. (Source)

Department Of Agriculture Official Sentenced To Prison For Bribery For Preferential Treatment In The Award Of $19 Million Of Security Contracts - August 10, 2021

Richard Holman, the former Chief of the U.S. Department of Agriculture (USDA) Office of Homeland Security and Emergency Coordination, Physical Security Division, was sentenced today to 180 days of home detention and fined $110,000 for carrying out a multi-year scheme in which he accepted bribes in exchange for ensuring the awarding of USDA contracts.

According to court papers, between July 2013 and December 2015, Eric Schneider and Communications Resources, Inc. (CRI) gave Holman and other USDA officials Corvette wheels, concert tickets, PGA tour tickets, meals, alcohol, strip clubs, parking, concierge medical services, prescription drugs, and other cash tips. In exchange, Holman gave Eric Schneider and CRI preferential treatment in the award of USDA contracts worth over $19 million. As part of the scheme, CRI employees drafted procurement documents in such a way as to favor the award of a multi-million dollar contract to CRI, and USDA officials used the documents in the procurement process as if they prepared them. (Source)

29 Individuals (Government & Business) Involved In $400,000 Conspiracy To Defraud The Department Of Agriculture - October 29, 2020

This scheme involved former federal, state, and local officials and prominent business people.

Federal prosecutors are close to finishing their work in bringing to justice dozens of current and former federal, state, and local officials and prominent business people all connected in a scheme to defraud the United States Department of Agriculture (USDA).

In November 2019, a federal grand jury returned a far-reaching indictment charging a County Executive Director of the United States Department of Agriculture's Farm Service Agency with orchestrating a broad-based conspiracy to steal government drought assistance funds and hide the actions through identify theft, tax evasion, and other federal crimes. As a result of this crackdown by U.S. Attorney Keefe's, 29 individuals were indicted; alleged to have defrauded the federal government, and taxpayers, of hundreds of thousands of dollars.

Duane Crawson led the conspiracy that included a former Holmes County Clerk of Court and numerous other individuals who had served in positions of public trust. Between May and December of 2017, while employed as a County Executive Director of the USDA's Farm Service Agency for Bay, Holmes, and Washington counties, Crawson devised a kickback scheme in which he and his co-conspirators unlawfully obtained approximately $400,534 in taxpayer funds by submitting fraudulent drought assistance claims.

Crawson submitted fraudulent claims for livestock and farmland parcels that were not actually owned or leased by the conspirators, resulting in drought assistance funds being deposited into the conspirators' bank accounts. The co-conspirators paid Crawson a portion of the fraud proceeds in the form of cash kickbacks. (Source)

U.S. FEDERAL RESERVE BOARD (FRB)

Federal Reserve Board Employee Pleads Guilty To Theft Of Restricted Government Documents Prior To Quitting Job - March 19, 2021

In 2019, the Federal Reserve Board (FRB) notified Venkatesh Rao that it considered his work performance to be unsatisfactory and Rao made a decision to voluntarily separate from the Board.

Over the course of five weekend days in November 2019, Rao entered the FRB building in Washington, D.C. approximately 16 times and printed more than 50 restricted government documents from his workstation and avoided FRB restrictions on the emailing and electronic copying of restricted materials. Rao removed the restricted documents, which contained proprietary information used by the FRB to conduct bank stress tests, from the FRB building and stored the materials at his home. (Source)

U.S. FISH & WILDLIFE

Fish & Wildlife Service Employee Charged With Embezzling $100,000+ - March 3, 2023

A federal grand jury in Alaska returned an indictment charging a Fairbanks U.S. Fish and Wildlife Service (USFWS) employee with wire fraud and embezzlement of public funds for perpetrating a years-long scheme to steal money from her employer.

Kimberly Robinson was employed with the U.S. Fish and Wildlife Service (USFWS) since 2003, and in 2020 was promoted to the role of Budget Analyst in charge of reconciling the budgets for each USFWS regional office. To perform her duties the federal government issued Robinson multiple credit cards to pay for official government expenses and travel.

From at least 2018 through June 2021, Robinson engaged in a scheme to defraud the U.S. Fish and Wildlife Service by using her government issued credit cards for unauthorized personal purchases and expenses. She then deleted and altered the unauthorized transactions on the credit card statements submitted to her supervisor for reconciliation to conceal the scheme and to cause USFWS to disburse public funds to pay the credit card balances.

Robinson embezzled over $100,000 through this scheme. (Source)

U.S. FORESENT SERVICE

U.S. Forest Service Employee Arrested For Accepting $360,000+ In Bribes And Kickbacks For 4 Years - March 1, 2021

Francisco Isaias who was a United States Forest Service employee.

He was arrested and charged with illegally directing nearly $900,000 in no-bid Forest Service vehicle repair and maintenance work to a San Bernardino County auto body repair shop that illicitly paid him more than $360,000 in bribes and kickbacks. (Source)

U.S. GEOLOGICAL SURVEY (USGS)

Geological Survey Employee Charged With Making 1.2 Million+ Of Un-Authorized Purchase For Personal Use - September 4, 2024

James Montoya worked as a federal employee at the United States Geological Survey (USGS) office in Lakewood, Colorado. USGS is part of the United States Department of the Interior (DOI).

During a routine initiative to identify misuse, DOI identified numerous questionable transactions on Montoya's government charge card. The indictment alleges that Montoya concealed these improper purchases by altering documents to indicate these purchases were for work-related items. The alleged actions defrauded the government of approximately $1,223,009.42 over approximately fifteen years beginning around December of 2008 and continuing through at least November 2023. (Source)

U.S. POSTAL SERVICE (USPS)

USPS Mail Carrier Sentenced To Prison For Stealing Credit Cards From Mail And Making $27,000 In Charges - January 10, 2025

Lakeatra White stole credit cards belonging to two victims, in which she tried to rack up personal charges estimated at nearly $27,000. During the investigation, White turned over 115 pieces of mail she had stolen to law enforcement. (Source)

USPS Employee Sentenced To Prison For Stealing 47 U.S. Treasury Checks Totaling $750,000+ - December 27, 2024

Zerion Franklin was a United States Postal Service employee at the mail processing annex in Fayetteville, North Carolina.

In June 2024, the Fayetteville Police Department conducted a traffic stop of Franklin's vehicle. After observing drug paraphernalia in plain view, officers conducted a search of the vehicle. During the search, officers located 47 U.S. Treasury checks made payable to entities and individuals other than the defendant. The checks, which were dated between April and May of 2023, included federal tax refunds, VA benefits, and social security disability benefits. Officers also located marijuana packaged for sale, a loaded 9mm handgun, and over $22,000 in U.S. currency.

Shortly after the traffic stop, an elderly victim in New Hanover County reported the theft of her tax refund check. It was later revealed that the check was stolen from the mail stream, altered to reflect Franklin's name as the payee, and cashed at a Walmart in Fayetteville on or about May 3, 2023. In total, investigators determined that Franklin stole U.S. Treasury checks totaling over $750,000. (Source)

USPS Supervisor Accused Of Stealing 90 Checks From Mail - December 26, 2024

On Oct. 31, 2023, Benita Randle stole about 90 checks from mail that had been entrusted to the Postal Service for delivery.

Randle was a supervisor at the St. Louis Processing and Distribution Center in St. Louis at the time. (Source)

USPS Manager Charged With Stealing $81,000+ Of Stamps - December 21, 2024

Emilio Chirico, the Station Manager for the DeWitt, New York Post Office, has been charged by indictment with wire fraud, misappropriation of postal funds, and false entries and reports

Between January 2021 and March 2023, Chirico stole $81,553.94 in stamps from the DeWitt Post Office and falsified postal records to conceal the theft of the stamps. Chirico has been the station manager at the DeWitt Post Office since March 2012. (Source)

USPS Employee Guilty Of Delaying And Stealing Contents Of U.S. Mail - December 13, 2024

Between on or about July of 2022, through October 4, 2022, Randy Brown unlawfully detained, and delayed U.S. mail, entrusted to him as a postal employee; and on September 26, 2022, September 27, 2022, and October 3, 2022, Brown did knowingly embezzle, steal and remove checks from U.S. mail, entrusted to him as a postal employee. (Source)

USPS Employee Convicted Of Threatening To Shoot And Kill Employees Of The New York State Department Of Labor - December 13, 2024

Quadri Garnes was employed as a mail carrier for the United States Postal Service (USPS) at the Homecrest post office in Brooklyn, New York, from March 26, 2022 to May 29, 2022.

After crashing his postal truck into two vehicles, Garnes was terminated on May 31, 2022. Garnes subsequently applied for unemployment benefits but was denied because he had worked for the USPS for fewer than 60 days and was thus ineligible to receive benefits. On the morning of September 29, 2022, Garnes called the New York State Department of Labor (DOL) and was advised that he had worked for the USPS for too short a period to be eligible to receive benefits. In response, he threatened to shoot and kill employees of the USPS and DOL. During the 45-minute recorded call with two DOL employees.

Garnes's Statements Included:

- If I go back to the post office, I'm gonna shoot somebody.
- Y'all gonna make me go to jail for killing somebody.
- Do the city want me to kill five or six different people?
- I got 18 and a half years in jail. It don't bother me to be in jail. I made myself, meaning like I'm made, as long as I'm in the New York City jail, I'm good.
- You might see this s--t on TV. Just remember my name. You might see it on TV tonight. You, just remember my name!
- Somebody might get shot today coming out of Department of Labor.
- Believe me, I'll be at the New York State Department of Labor down on Schermerhorn or Livingston Street and I will make a big f----ng deal out of it.

Garnes's threats triggered an immediate response by the DOL, the New York State Police and by Postal Inspectors, who took precautions against Garnes's return to the postal facility where he had briefly worked and the DOL office he named. Garnes was arrested approximately two weeks after making his threats. (Source)

USPS Employee Sentenced To Probation For Mail Theft - December 12, 2024

Shakeitha Wiley was a mail handler at the New Orleans Processing and Distribution Center. Wiley opened a parcel of mail not directed to her and removed two gift cards totaling $210. Wiley later used the stolen gift cards for her own benefit. (Source)

USPS Employee Sentenced To Prison For Stealing $3,300 In Money Orders - December 11, 2024

Between on or about December 1, 2023, and April 16, 2024, Tiffany Isenhart stole $3,380 in money orders while employed at the Charmco Post Office in West Virginia, and converted them to her own use. Isenhart admitted that she used her position as a United States Postal Service employee to issue the money orders to herself without paying for them or paying the associated fees. (Source)

USPS Human Resource Officer Pleads Guilty To Theft & Sale Of $6 Million+ In Checks - November 13, 2024

On several occasions from October 2023 to April 2024, Ahmad Omar Shareef, a former U.S. Postal Service Human Resource Officer at the Bloomfield Post Office in Pennsylvania, removed and stole business checks contained in U.S. mail addressed to Pittsburgh area businesses.

Shareef then used an encrypted messaging app to sell the checks to buyers in other cities. This mail included more than 450 checks recovered from Shareef and his property that were addressed to businesses in Pittsburgh area neighborhoods and that totaled more than $6 million. Nearly $250,000 of that total was fraudulently negotiated by buyers, with Shareef admitting to earning an estimated $20,000 through the scheme. (Source)

USPS Manager Who Stole Drugs From Mail, Shared With Co-Worker Sentenced To Prison On Drug & Gun Charges - October 25, 2024

On multiple occasions between May 2018, and May 2, 2022, Ralph Minni used his position as the post office station manager to take parcels containing controlled substances, such as marijuana, out of the mail stream and into his private office, remove the contents, and then return the empty packages back into the mail stream.

Minni then transported the controlled substances to his residence, where he would store and redistribute the narcotics to other individuals. On three occasions in March and April of 2022, Minni distributed quantities of cocaine to a coworker, who then proceeded to snort the cocaine off Minni's office desk in his presence. On May 2, 2022, a search warrant was executed at Minni's residence during which investigators recovered quantities of marijuana, approximately 700 grams of cocaine, approximately 40 firearms, and over 19,000 rounds of ammunition. Minni was arrested that same day after leaving the Greece Post Office. Officers recovered a quantity of marijuana from inside his vehicle, which he had removed from a mailed package and planned to take back to his residence for subsequent sale and distribution. (Source)

USPS Service Employee Arrested For $10,000 COVID Relief Fraud - October 23, 2024

During the COVID pandemic, the United States Small Business Administration (SBA) offered Targeted Economic Injury Disaster Loan (EIDL) Advances that did not need to be repaid. The advances were for small businesses that were in low-income communities and received a reduction in revenue of more than 30% during an eight-week period.

Between June 28 and 30, 2020, Brooks Stewart devised a scheme to defraud the SBA by electronically applying for an EIDL advance and providing false representations in her application. Afterwards, she fraudulently received a $10,000 EIDL advance. (Source)

USPS Employee Sentenced To Prison For Stealing $5,000 Worth Of Cash & Gift Cards From Mail - October 9, 2024

Justin Crain was employed as a U.S. Postal Service Mail Processing Clerk at its Indianapolis Processing and Distribution Center.

The Postal Service's Office of Inspector General began an investigation after it identified numerous mail items that passed through the Indianapolis processing center and had been opened before being delivered to their intended recipients. Video surveillance captured Crain opening numerous greeting cards and removing cash and gift cards from inside.

Over the course of just two hours, Crain was seen dozens of times rifling through mail items attempting to find cash. Crain was interviewed by investigators and admitted to stealing approximately $5,000 over the course of a few months. (Source)

USPS Mail Carrier Indicted For Throwing Baskets Of Mail Into A Trash Dumpster - October 3, 2024

On August 3, 2024, DuJuan Butler was driving a U.S. Postal Service truck while delivering the mail in Antioch, Tennessee.

A woman happened to look out her window and saw Butler take baskets of mail from the Postal truck and throw them into dumpsters behind a strip mall. The woman filmed Butler and then uploaded her video to TikTok where it was viewed millions of times. Other Postal Service employees were later able to recover the discarded mail from the dumpsters. (Source)

USPS Employee Admits To Stealing $24,000+ Of Money Orders - October 3, 2024

Tanya Lee Holbrook began working as a postmaster of the Gardiner post office in Montana in September 2022.

In February 2023, the manager of postal operations in Montana contacted the U.S. Postal Services Office of Inspector General regarding concerns that Holbrook was stealing office bank deposits.

An investigation determined that Holbrook routinely issued money orders to herself and others but did not submit the funds for them to USPS. Between November 2022 and September 2023, Holbrook delayed approximately 48 bank deposits, totaling $46,755, from the Gardiner post office. While Holbrook usually sent the cash later when she was paid, she never provided funds for eight deposits, which totaled $24,443, from January 2023 to September 2023. When interviewed, Holbrook confessed to the thefts. Holbrook stated that she issued herself or family member's money orders without remitting payment and then delayed sending the funds. Holbrook eventually fell so far behind that she was unable to pay for several deposits. (Source)

USPS Employee Accused Of Stealing $1.5 Million Checks From Mail And With $20,000+ Of COVID Pandemic Protection Program Fraud - September 26, 2024

Anthony Virdure worked at the Postal Service Processing and Distribution Center at 1720 Market Street in St. Louis, Missouri. He had access to all first-class mail routed through the center.

Virdure is accused of stealing checks with a face value of more than $1.5 million from the mail.

The indictment also accuses Virdure of fraudulently applying for and receiving a $20,832 Pandemic Protection Program (PPP) loan in 2021 for a tobacco store called Virdure Dynamics.

The loan application contained false information about the business' income and Virdure supplied a false IRS Schedule C in support of the application, the indictment says. The purported address of the store was actually his grandmother's house, it says. (Source)

USPS Mail Carrier Convicted Of Receiving Bribes, Fraud Conspiracy & Drug Conspiracy - August 20, 2024

Emerson Pavilus was a mail carrier at the post office in Flanders, New Jersey.

From at least 2015 to 2020, Pavilus received cash payments in exchange for helping individuals intercept packages containing illegal narcotics and other illicit materials. Pavilus provided his conspirators with addresses for vacant houses along his mail route to which they could ship illegal packages. Pavilus then intercepted those packages from the mail stream and personally delivered them to his conspirators in exchange for bribe payments at places other than the addresses listed on the packages. (Source)

USPS Maintenance Manager Sentenced To Prison For Stealing $6,500 In Cash - July 26, 2024

Barry Gallon was employed as a Maintenance Manager at the United States Postal Service's Indianapolis Processing and Distribution Center for seven years.

Between August 31, 2023, and September 20, 2023, Gallon stole cash from letters, packages, bags, and mail while working at the distribution center. The total amount of money stolen by the defendant was found to be no more than $6,500. (Source)

2 USPS Workers Charged With Stealing U.S. Treasury Checks Valued At $4 Million+ - July 10, 2024

Between June 2021 and August 2023, Kevaughn Wellington and Ky-Mani Straker (USPS Employees) engaged in a scheme to steal and sell Treasury checks intended for, among other things, individuals entitled to Social Security benefits, COVID-19 stimulus checks and tax refunds. Wellington stole parcels containing Treasury checks from the JFK Mail Facility where he was employed at the time as a postal worker. Then, together with Straker and others, Wellington sold the stolen Treasury checks for a cut of the profit.

As part of the scheme, Wellington and Straker stole over 125 Treasury checks valued at more than $4 million. Straker falsely endorsed and deposited stolen Treasury checks in a bank account and withdrew the deposited funds for his own financial gain. (Source)

USPS Employee Sentenced To Prison For Stealing $90,000 Worth Of Money Orders - June 11, 2024

Jamesa Rankins worked as a Sales & Service Distribution Associate at the Montello Post office in Brockton, Massachusetts for approximately four and a half years.

Prior to her termination in January 2021, Rankins had the ability to generate postal money orders, including replacement money orders. Customers could obtain replacement money orders without paying any additional fees if the original postal money orders were lost, damaged or erroneous. Beginning around September 2020, Rankins issued approximately 126 fictitious replacement money orders to an associate for money orders that were not lost, damaged or erroneous. In many instances, the fictitious replacement money orders actually invalidated properly issued money orders. In total, Rankins issued nearly $90,000 worth of replacement money orders.

Beginning in May 2020, Rankins also applied for and obtained Pandemic Unemployment Assistance from the Massachusetts Division of Unemployment Assistance despite being employed by USPS and thus being ineligible to receive unemployment assistance. In total, Rankins collected at least $15,000 in unemployment benefits to which she was not entitled. (Source)

USPS Employee Charged With Stealing Ten Of Thousands Of Dollars Worth Of Checks From Mail & For Fraud - Identity Theft Scheme - June 7, 2024

Kierra Blount while employed by the U.S. Postal Service in Stamford, Connecticut stole mail and obtained stolen mail for the purpose of obtaining checks that were payable to other individuals.

In approximately November 2021, Blount opened a bank account using the name and social security number of an individual without the identity theft victim's knowledge. Blount and others fraudulently changed the payee names on stolen checks to the name of the identity theft victim, forged the victim's signature on the back of the checks, and deposited them into the bank account Blount opened. From November 2021 until the account was closed in April 2022, Blount and others deposited tens of thousands of dollars in fraudulent checks into the account. They then used the funds for their own purposes. (Source)

USPS Service Mail Carrier Sentenced To Prison For Role In $129,000+ Check Fraud Scheme - May 3, 2024

Alexus Tyson was a United States Postal Service (USPS) Mail Carrier.

Tyson participated in a conspiracy whereby she used her position as a USPS) mail carrier to wrongfully access checks, money orders, and personal mail put into the mail by victims. That information was then used by a co-conspirator, Travis Nnamani, to create counterfeit checks to take money from victims' bank accounts.

Between August 2019 and October, 2020, Tyson assisted Nnamani to create fraudulent checks using victims' personal information that Tyson and others at the USPS took from checks and other documents that victims placed into the mail system. In many instances, checks or other documents mailed by victims were photographed by Tyson or other USPS employees and then the documents were put back into the mail with the victims not knowing their information had been stolen. That information would then be used by Nnamani to create false checks using that information to access funds in victims' bank accounts.

Tyson also played a role as a recruiter of other employees at the USPS to engage in similar conduct, including selling federal stimulus checks they took from the mail. (Source)

USPS Employee Charged With Embezzling $19,000+ / Gave Funds To Boyfriend & Family Members - March 22, 2024

Christine Hedges began working for USPS around 2020, most recently as a Lead Sales & Service Associate in Brockton.

It is alleged that from approximately October 2021 to August 2023, Hedges engaged in a scheme to steal USPS funds for her personal use. As part of this scheme, Hedges allegedly generated, for her own use, no-fee money orders without a customer physically present at her customer window and which a customer did not request. Hedges also allegedly stole cash from her USPS workstation and often attempted to conceal her theft by replacing the cash with these fraudulent money orders. Hedges allegedly generated approximately 70 fraudulent no-fee money orders. 11 of those no-fee money orders were made out to her boyfriend or a family member.

From on or about Aug. 1, 2023 to on or about Aug. 14, 2023, video surveillance from above Hedges' workstation allegedly showed Hedges on at least one occasion removing cash from her assigned drawer and putting it in her pocket. In all, Hedges allegedly embezzling over $19,707 in postal funds. (Source)

4 USPS Mail Carriers Charged For Delay Of 40 Pieces Of Election Mail - March 14, 2024

In September 2022, the Puerto Rico State Elections Commission (Commission) conducted a Special Election for the San Juan, Puerto Rico District 1 Senate vacancy. As part of the Commission's services provided for the Special Election, in August 2022, the Administrative Board of Absent Voting and Early Voting ("Junta Administrativa de Voto Ausente y Voto Adelantado" ("JAVAA")) mailed ballots to certain eligible voters in Puerto Rico, via USPS certified mail service.

Four individual mail carriers, employed by the USPS, delayed and did not deliver a total of forty pieces of election mail from the September 2022 Special Election to domiciled active voters in San Juan. (Source)

USPS Employee Sentenced To Prison For Stealing Mail Over 4 Years - March 5, 2024

Pamela Jo Rosas pleaded guilty to theft of mail by a postal employee and was sentenced to 37 months.

In April 2020, postal inspectors began receiving complaints that a series of parcels containing valuable coins were missing after being placed in the post office for delivery. Federal agents conducted surveillance and identified a postal employee, Pamela Jo Rosas, as a subject involved in the theft after viewing her handling packages in a suspicious manner. Rosas was also found in possession of several pieces of stolen mail packages after leaving work. Rosas admitted to stealing many items from the post office during the previous three to four years. Agents were able to recover hundreds of valuable coins from her apartment, along with other items Rosas had stolen from the mail during the course of her employment. (Source)

USPS Mail Carrier Admits To Receiving $156,000+ Of Disability Payments While Working As The Owner Of His Travel Agency - January 30, 2024

Pamela VanSyckle worked for the U.S. Postal Service as a rural carrier.

In September 2020, VanSyckle signed and filed a claim form alleging that she sustained an injury at work. Thereafter, she signed and filed multiple federal claim forms alleging that she had not worked or had outside employment for extended periods of time. Based on the submission of those claims, VanSyckle received $156,872 in disability payments from the federal government.

During the time in which she received disability benefits, VanSyckle was in fact working as the owner and operator of a travel agency. While alleging in her claim forms that she was neither self-employed nor involved in any business enterprise, VanSyckle performed a variety of services for the travel agency including sales, marketing, and financial operations. (Source)

USPS Employee Sentenced To Prison For Stealing $2,400+ Of Money Orders - December 13, 2023

While working for the USPS in Ithaca, New York, Stephen Perrine stole 10 money orders totaling $2,480, by issuing them to himself and entering fraudulent justifications in a USPS accounting system. (Source)

USPS Mail Carrier Admits To Stealing $170,000+ In Cash From Mail - December 1, 2023
From November 2021 to August 2022, Joseph Fenuto was employed as a U.S. Postal Service letter carrier.

Fenuto admitted he had stolen more than 50 such parcels containing cash from numerous retail stores at the Gloucester Premium Outlets. Fenuto said he stole $171,110 from parcels that he was required to ensure remained in the mail stream for their delivery to a bank. (Source)

USPS Worker Sentenced To Prison For Stealing $18,000+ - December 1, 2023
From August 2018, Zeon Johnson worked as a Sales and Service Distribution Associate for USPS. As part of his job, Johnson sold stamps and processed money order transactions for USPS customers.

From approximately July 2019 through June 2020, Johnson converted over $18,000 in USPS funds for personal use by stealing cash funds paid by customers for stamps and issuing USPS money orders payable to himself. (Source)

USPS Employee And 2 Co-Conspirators Arrested For $24 Million+ Stolen Check Scheme - November 17, 2023
From March 2021 to July 2023, Nakedra Shannon was employed by the U.S. Postal Service (USPS) as a mail processing clerk at a USPS processing and distribution center in Charlotte, NC.

From April to July 2023, Shannon conspired with Donnell Gardner and Desiray Carter to steal incoming and outgoing checks from the U.S. mail, which Gardner and Carter then sold to other individuals including using the Telegram channel OG Glass House. Over the course of the conspiracy, the co-conspirators allegedly stole checks totaling more than $24 million, including more than $12 million in stolen checks which were posted for sale on the Telegram channel OG Glass House, and more than $8 million in stolen U.S. Treasury checks. The indictment also alleges that the defendants obtained hundreds of thousands of dollars in criminal proceeds of the mail theft scheme. (Source)

USPS Employee Convicted For Stealing & Selling Master Mailbox Key For $2,500 - November 17, 2023
Kristen Williams was employed as a mail carrier at the post office in Alabama

In late October 2022, Williams stole and sold a USPS arrow key to a coconspirator. Arrow keys are government property and will open all blue USPS collection boxes in a particular geographic area. Williams's coconspirator, who previously pleaded guilty to bank fraud conspiracy and aggravated identity theft, paid Williams $2,500 in cash for the key. Law enforcement caught Williams's coconspirator using the key to steal mail from collection boxes outside a mall in November 2022. The coconspirator stole hundreds of pieces of mail using the key.

Williams also conspired to commit bank fraud involving counterfeit checks deposited into her bank account. The counterfeit checks were derived from checks stolen from the mail. (Source)

USPS Employee Worker Charged For Role In Stealing Business Checks Worth Over $1.9 Million From Post Office - October 21, 2023

From November 2022 to April 2023, Dontavis Truesdale worked as a Processing Clerk at the Ballantyne Post Office in Charlotte Noth Carolina.

Truesdale used his position as mail processing clerk to steal hundreds of checks of businesses that maintained post office boxes at the post fffice. Truesdale sold the stolen checks to other co-conspirators who committed bank fraud, by depositing the stolen checks into bank accounts they controlled, and then quickly removed the funds before the banks detected the fraud. Truesdale stole more than 200 checks with a total face value of over $1.9 Million. (Source)

USPS Employee Admits To Defrauding The USPS Of $874,000+ - October 16, 2023

Ephrem Nguyen was employed by the U.S. Postal Service (USPS) as the Postmaster of the Danbury Post Office in Danbury, Connecticut .

His responsibilities that included supervising the maintenance and repair of all equipment, facilities, and vehicles assigned to the post office. In November 2020, Nguyen required that all Danbury Post Office vehicle maintenance and repair work be performed by a certain vendor, even though Nguyen knew that another vendor already had a contract for with the Danbury Post Office for those services. Nguyen demanded that the vendor provide free vehicle maintenance and repairs for himself, one of his children, a USPS employee, and employee of Nguyen's personal business. In 2022, Nguyen solicited and received $90,000 in cash bribes from the vendor. In exchange for these bribes, Nguyen caused the USPS to overpay the vendor for vehicle maintenance and repair, which Nguyen characterized as a "raise." Between approximately January 2022 and February 2023, Nguyen used USPS credit cards to pay the vendor more than $1 million, or approximately $760,000 more than necessary to pay for legitimate maintenance and repair work.

In addition, Nguyen embezzled more than $80,000 from the USPS by using his USPS credit cards to rent vehicles for the personal use of himself and others, and he approved more than $8,000 in fraudulent travel expense reimbursement claims for a co-worker.

Through these schemes, Nguyen defrauded the USPS of approximately $874,930.59. (Source)

USPS Employee Charged With Stealing $1.6 Million+ Of Checks From Mail - September 22, 2023

Between October 2021 and March 2023, Hachikosela Muchimba was an employee of the U.S. Postal Service.

Muchimba executed a scheme to steal checks from the U.S. mail and direct those funds into a bank account under his control. Muchimba would remove the name of the proper payee and replace it with his own name. Many of these misappropriated checks were U.S. Treasury checks. He is seen on bank surveillance removing the proceeds from ATM machines.

The total amount of the checks that were fraudulently deposited into Muchimba's accounts was $1,697,909.52. Law enforcement executed a search warrant at Muchimba's personal residence on March 29, 2023. In the course of that search, law enforcement recovered an ATM receipt that reflected a deposit of a U.S. Treasury Check in the amount of $415,173.53. (Source)

USPS Employee Admits To Stealing Stimulus Checks From the Mail - September 18, 2023
Olivia Bryant admitted in a plea agreement that in 2020 and 2021 she stole hundreds of pieces of mail from her route in Chicago's Logan Square neighborhood.

Some of the stolen mail contained government stimulus checks that were issued by the U.S. Treasury during the Covid-19 pandemic. Bryant admitted that five of the stimulus-check thefts occurred on St. Patrick's Day 2021 when she removed the checks from her postal satchel and transferred them to her purse. (Source)

USPS Mail Carrier & Husband Plead Guilty For $8.8+ Million Mail Theft Scheme - September 15, 2023
Kiara Padgett was employed by the U.S. Postal Service as a Mail Carrier with a postal route in West Charlotte, NC.

From August 2021 to November 2022, Padgett used her position as a Postal Carrier to steal incoming and outgoing checks of businesses and individuals. Padgett sold the stolen checks to Dominique Dunlap her husband, using Dunlap as her intermediary to other individuals, including to Terrell Alexander Hager, Jr. The total face value of the checks stolen by Padgett was over $8.8 Million.

Dunlap negotiated with Hager, Jr. about the sale of stolen checks over text messages, and sent Hager, Jr. photographs of stacks of stolen mail and of stolen checks of victim companies on Padgett's postal route.

In March 2023, Hager, Jr. pleaded guilty to conspiracy to commit bank fraud. Between August 2021 and November 2022, Hager, Jr. and other individuals obtained stolen checks from Padgett through Dunlap. Hager, Jr. and his co-conspirators deposited the stolen checks into bank accounts they controlled, and then made cash withdrawals before the financial institutions detected the fraud. Over the course of the scheme, Hager, Jr. and his co-conspirators deposited more than $66,000 in stolen checks and money orders. Hager, Jr. also posted online for sale more than 400 stolen checks totaling over $7.3 million. The checks posted by Hager, Jr. were stolen from Padgett's postal route in West Charlotte. At the time Hager, Jr. committed this fraud, he was on probation with the state of North Carolina for an unrelated offense. (Source)

USPS Employee Sentenced To Prison For Role In $2 Million COVID Relief Fraud Ring - August 17, 2023
Tiffany McFadden was a U.S. Postal Service employee.

McFadden was the leader of a scheme responsible more than 400 fraudulent Paycheck Protection Program PPP loan applications.

McFadden and her co-conspirators manufactured false and fraudulent documents claiming businesses that in truth did not exist and did not lose money due to the COVID-19 pandemic. As a result, McFadden and others received more than $2,000,000 in loans, often approximately $20,000 at a time, that they were not entitled to. Those loans were later fully forgiven by the U.S. Government.

McFadden and others recruited loan applications by word of mouth, manufactured false and fraudulent tax and business documents, and then applied for and obtained forgiveness for the loans. In exchange for her services, McFadden received a portion of the fraudulently obtained funds. (Source)

USPS Mail Carrier Who Was On Administrative Leave Sentenced To Prison For Stealing Mail From 900 Customers - August 11, 2023

During the evening of November 21, 2022, an off-duty San Diego Police detective saw a woman in a hooded sweatshirt open a communal mailbox at his apartment complex in Santee, California and remove multiple pieces of mail. As the detective approached, the female closed the mailbox and fled in a White Nissan. After getting the license plate of the vehicle, the detective determined that Rumley resided at the same address as listed for the vehicle registration and referred the matter to the U.S. Postal Service.

Rumley had been placed on administrative leave from her employment at the Santee Post Office earlier that month and was terminated by the Postal Service on December 12, 2022.

After securing a search warrant for the residence, on December 21, 2022, United States Postal Service Inspectors found more than 1,500 pieces of mail in Rumley's residence including, but not limited to, gift cards, credit cards and even several Christmas presents that had all been stolen from nearly 900 customers along her mail delivery route in Santee. Inspectors also found the keys she was given as a mail carrier to access mailboxes. The keys were hidden in a potted plant within her bedroom. In her plea agreement, Rumley admitted that, even after being placed on administrative leave, she kept those keys though she was not authorized to do so and used them to continue to steal mail even after she was terminated. (Source)

USPS Mail Carrier & Co-Conspirator Sentenced To Prison For $244,000+ Identity Theft / Fraud Scheme Using Stolen Mail - August 9, 2023

Robenson Fenelon and Squille Traxler, have been sentenced to prison after pleading guilty to conspiracy to commit bank fraud and theft of stolen mail. Fenelon additionally plead guilty to aggravated identity theft.

From at least January 2019 through December 2020, Fenelon and Traxler conspired with mail carriers in a scheme to steal the identities of at least 50 victims, and used that information to defraud financial institutions of a total of $244,222.93.

Traxler was employed as a Mail Carrier with the U.S. Postal Service. Fenelon recruited Traxler to assist in identifying potential identity theft targets. Fenelon and Traxler used Traxler's access to the mail to obtain the targets' identity information, including names, dates of birth, social security numbers, addresses, phone numbers, and bank account numbers. Fenelon then used that information to access and take over the victims' bank accounts or to open new bank accounts in the victims' names.

Fenelon contacted the victims' banks, purporting to the victims or their relatives, and requested a new debit or credit card for the victim's account. For the newly established accounts, Fenelon applied online or over the phone for new accounts and credit cards. Fenlon and Traxler then stole the credit cards from the victims' mail. Fenelon and Traxler used the cards to withdraw cash and make personal purchases. They stole checks from the mail and deposited them into the bank accounts they controlled. (Source)

USPS Mail Carrier Charged For Role In Stealing $40,000+ In Checks / Money Laundering - July 24, 2023

From at least May 2021 Jakia McMorris was an employee of the U.S. Postal Service (USPS), working as a city carrier at the North Tryon Station in Charlotte, North Carolina.

Around September 13, 2021, McMorris reported that, while she was delivering mail, she lost a USPS universal key that could open many U.S. mailboxes. After that day, McMorris allegedly stopped reporting for work at the USPS.

Beginning in September 2021, McMorris and her co-conspirators executed a scheme to commit bank fraud by stealing more than $40,000 in checks, including from the U.S. mail. The indictment alleges that the co-conspirators used stolen universal USPS keys to open multi-unit outdoor mailboxes in Charlotte and steal mail. The stolen mail included business checks.

As part of the scheme, the indictment alleges that the co-conspirators deposited the stolen checks into bank accounts they controlled, including in bank accounts in McMorris's name. It is alleged that the co-conspirators then quickly withdrew the cash from the accounts before the banks detected the fraud. McMorris allegedly received a portion of the funds as payment for using her bank accounts to perpetuate the scheme.

As part of the conspiracy, the indictment also alleges that the co-conspirators attempted to disguise the payments made to the defendant by using the fraudulent proceeds in McMorris's bank account to purchase money orders, which McMorris then deposited back into her bank accounts. (Source)

USPS Employee Pleads Guilty To Using Her Position To Obtain The Personal Information Of Victims As Part Of Conspiracy To Commit Bank Fraud / Wire Fraud - - June 6, 2023
Breanna Cartledge was a Clerk with the U.S. Postal Service (USPS).

Cartledge pleaded guilty to conspiracy to commit bank fraud and wire fraud, in connection with a scheme to defraud financial institutions by creating fake checks using information Cartledge collected.

Cartledge wrongfully accessed USPS money orders and individual mail to illegally obtain the personal information of victim individuals and businesses, which she and her co-conspirators used without the victims' authorization.

For example, after a co-conspirator texted Cartledge requesting pictures of checks, Cartledge sent the co-conspirator images of at least nine separate money orders or checks that contained personal identifying information with the intent that the information be used to create fake checks to steal from victim accounts.

Cartledge negotiated a counterfeit check fraudulently drawn for $4,900 from the account of a victim, but the transaction was reversed by the bank. Cartledge admitted that she abused her position as a USPS Clerk to facilitate the commission or concealment of the offense. (Source)

USPS Mail Carrier Sentenced To Prison For Role In Distributing Cocaine Packages - May 24, 2023
Michelle Prieto is a former United States Postal Carrier.

Prieto and her co-defendant, Angel Coss, orchestrated a scheme by which Prieto provided addresses on her delivery route to Coss who used those addresses to secure shipments of cocaine from Puerto Rico. As a result, kilogram quantities of cocaine were shipped in packages to these addresses. Prieto then removed the packages from the mail stream and provide them to Coss who then distributed the cocaine. (Source)

USPS Supervisor Charged With Misappropriation of $65,000 Of Postal Funds For Personal Use - May 17, 2023

Austin Mahan is charged with misappropriating approximately $65,000 in postal funds.

For approximately six months in 2022 and 2023 Mahan worked as a U.S. Postal Service (USPS) Supervisor.

At various times Mahan misused USPS credit cards to make personal purchases at various retail stores in and around New Jersey. These purchases included tens of thousands of dollars' worth of gift cards as well as various home décor items, home renovation materials, power and handheld tools, tool storage equipment, and personal items such as a Dyson cordless vacuum, LED fog light bulbs for Mahan's personal vehicle, batteries, shampoo, shaving cream, food products and other items. (Source)

USPS Employee Sentenced To Probation For Misappropriation Of USPS Funds / Used Funds For Herself And Family - May 10, 2023

Megan Torrez was employed by the U. S. Postal Service in June 2021, as a Postal Support Employee in Nelson, Wisconsin. Her assigned duties included conducting postal business with the public and performing financial accounting functions to report the sales of postage, money orders and other items. When postage and money order stock were sold, she was responsible for collecting money from those sales and remitting that money to the bank.

Between August 2021 and February 2022, Torrez manipulated postal funds accessible to her in her position at the post office by issuing postal money orders to herself and family members and paying with personal checks that she admitted had insufficient funds to clear her bank. Postal money orders may only be purchased with cash, debit card, or traveler's check, and no personal checks are accepted by the Postal Service.

In January 2022, the Office of Inspector General received information about the checks written by Torrez to the Postal Service that were returned as "non-sufficient funds." At the time of their investigation, thirty-two checks were outstanding for over $26,000 in postal money orders. The money orders that Torrez issued to herself and her family were used to pay for her family's personal expenses. Torrez claimed that her decision to use postal funds to pay for her family's bills was out of desperation when her husband lost his job during the pandemic. (Source)

USPS Mail Carrier Sentenced To Prison For Role In Stealing $200,000+ From Her Mail Route Debit Cards Containing Public Benefits - April 24, 2023

From at least August 2015 to May 2020, Toshell Hunter schemed to defraud Bank of America by using her position as a USPS mail carrier to steal mail containing California Employment Development Department (EDD) debit cards that contained unemployment insurances benefits. Hunter also stole debit cards containing Economic Impact Payments for federally issued monetary relief because of the COVID-19 pandemic, United States Treasury checks, and other mail containing personal identifying information related to victims assigned to Hunter's mail route.

Hunter would then give the stolen EDD and other cards to co-defendant Michalea Barksdale who then activated and fraudulently used them. Hunter provided Barksdale the stolen debit cards in exchange for future payments and gifts.

Hunter helped Barksdale make fraudulent and unauthorized cash withdrawals from 68 separate victims' accounts and stole approximately $204,812 from Bank of America. (Source)

USPS Mail Carrier Sentenced To Prison For Teaching Other Mail Carriers How To Deliver Drugs Through Mail - March 30, 2023

Former USPS Mail Carrier Robert Sheppard was sentenced to prison for recruiting fellow mail carriers, and teaching them how to deliver packages of cocaine and marijuana while he was on disability leave.

In 2015, Sheppard worked as a U.S Postal Service (USPS) Mail Carrier. In exchange for receiving bribes, Sheppard used his position to deliver five-pound packages of drugs through the U.S. mail to Dexter Frazier, a local drug trafficker who sold cocaine and marijuana.

In 2016, Frazier approached Sheppard about delivering additional drug packages. Sheppard was on disability leave from the USPS at that time and unable to intercept and deliver packages.

But he offered to recruit other mail carriers to deliver drugs for Frazier in exchange for referral fees in the form of a mix of cash and marijuana. Frazier agreed to the arrangement.

Sheppard then contacted two coworkers, Tonie Harris and Clifton Lee. Sheppard explained to Harris and Lee that they could earn bribes for delivering packages of drugs along their mail routes, and taught them how to arrange the deliveries to avoid detection. Harris and Lee agreed to participate in the scheme, and Sheppard gave their phone numbers to Frazier. Frazier then coordinated the illegal deliveries with Harris and Lee. Harris and Lee each delivered three packages for Frazier believing they contained two kilograms of cocaine or 10 pounds of marijuana, per parcel. (Source)

USPS Employee Charged With Embezzling $52,000+ - March 27, 2023

Anthony Fernandes was a Supervisor for the USPS in Buzzards Bay, Boston.

Fernandes fraudulently used his USPS supervisor's travel authorization account to approve approximately $52,987 in bogus travel reimbursement requests for the period of April through November 2022. (Source)

USPS Mail Carrier Sentenced To Prison For $1,200+ Of Mail Theft - March 15, 2023

Diamante Williams was indicted by a federal grand jury on three counts of mail theft by a U.S. Postal employee in March 2022 for events which occurred in March and April 2018.

In September, 2022 as stated in William's plea agreement, on or about March 28, he stole mail and contents of mail from individuals residing on his route, including financial instruments. Williams admitted to stealing a check intended for company in the amount of $1,274. (Source)

USPS Employee Sentenced To Prison For Stealing $90,000+ Of Cash From Mail To Pay Off Debt / Give Money To Family - March 8, 2023

Roberta Feliz was employed as Lead Sales and Services Associate with the Gardner Post Office in Boston.

Between February and July 2020, Feliz stole over $90,000 in cash deposits that were mailed from a Tractor Supply Company to its bank. Feliz, who was scheduled to work on each day that a cash package was mailed, was observed on surveillance camera removing envelopes from the postal service floor into the employee locker area or the women's restroom.

In August 2020, Feliz was approached by law enforcement after she took a control package containing cash from the postal floor into an office, removed money from the envelope and hid it in an unused desk.

Feliz admitted to stealing packages from the Tractor Supply Company and stated that she used the money to pay off debt and sent some to family overseas. (Source)

USPS Employee Sentenced To Prison For Stealing Blank Money Orders Valued At Over $4 Million - January 4, 2023

In February 2021, 10,000 blank money orders were reported missing from a USPS post office on Utica Avenue in Brooklyn, New York where Jaleesa Wallace worked. The money orders can be deposited with a financial institution for up to $1,000 each.

Agents recovered over 3,000 of the stolen money orders from Wallace's residence. Over $4 million worth of the stolen money orders have been cashed at various financial institutions throughout the country.

Agents also recovered prepaid Department of Labor unemployment benefit cards and approximately $43,000 in cash from Wallace's apartment. Additionally, Wallace was in possession of approximately 42 pieces of mail from the Department of Labor that were not in her name.

Wallace was terminated by the USPS in August 2021. She forfeited the cash seized from her apartment to the United States Postal Inspection Service. A related defendant, Willie Cook, pleaded guilty to mail theft in March 2022 and is awaiting sentencing. (Source)

USPS Mail Carrier Pleads Guilty To Role In Stealing $145,000+ In Jobless Benefit Debit Cards From Mail - December 14, 2022

From January 2019 to May 2020, Toya Hunter stole mail, including letters with jobless benefit debit cards, sent by the California Employment Development Department (EDD), which administers the state's unemployment insurance program, which. Hunter then gave the stolen EDD debit cards as well as other credit cards and financial instruments to her co-schemer. The co-schemer then activated and fraudulently used the cards to commit bank fraud.

In March 2020, Hunter stole mail from her assigned route, including an EDD debit card belonging to a victim. Hunter also stole correspondence in the mail that contained the victim's name and the last four digits of the victim's Social Security number, which she later gave to her accomplice in exchange for cash and gifts, knowing the accomplice intended to activate and fraudulently use the victim's debit card.

Hunter's co-schemer used the debit card and the last four digits of the victim's Social Security number to fraudulently activate the card and create a personal identification number (PIN) to access funds from the victim's account, which was held at Bank of America. The co-schemer then used the victim's stolen EDD card to withdraw cash from a Bank of America ATM located in Corona.

During the scheme Hunter aided and abetted her accomplice in making fraudulent and unauthorized cash withdrawals from 68 separate victims' accounts and stole approximately $145,191 from Bank of America.

In July 2021, Hunter stole from the mail and fraudulently activated a stolen debit card containing COVID-19 pandemic unemployment relief money belonging to another victim. Hunter used the card to make fraudulent purchases and cash withdrawals, thereby stealing approximately $1,400 from Fiserv Bank. (Source)

USPS Mail Carrier Pleads Guilty To Stealing $2,700 Worth Of Gift Card, Cash, Jewelry From Mail - November 10, 2022

A former U.S. Postal Service Mail Carrier Breanna Wares pleaded guilty that she stole approximately $2,700 worth of gift cards, cash and jewelry from customers.

Wares stole these items from approximately 20 customers along her route near Camp Pendleton at the Brooks Street Station in Oceanside, CA.

The investigation determined that Wares unlawfully redeemed over 30 Target gift cards that had been placed in the mail, totaling more than $1,400. During a search of Ware's personal vehicle, agents discovered more than 40 gift cards valued at more than $1,300. Agents also found sheets of stamps, jewelry, foreign currency, rifled and unrifled First Class Mail greeting card envelopes. Agents also found a Trader Joe's gift card in Wares' wallet. (Source)

USPS Mail Carrier Pleads Guilty To Attempting To Bribe U.S. Postal Supervisor To Divert Packages Of Cocaine - November 2, 2022

John Noviello was a Mail Carrier for the U.S. Postal Service.

On Feb. 15, 2022, Noviello approached a U.S. Postal supervisor seeking their assistance in a scheme to divert postal packages suspected of containing cocaine. Noviello offered to pay the supervisor $1,750 per kilogram of cocaine successfully obtained from any diverted packages. On Feb. 17, 2022, Noviello left $850 in cash, concealed in a Dunkin' bag, inside the supervisor's vehicle in an attempt to encourage the supervisor to agree to the scheme. Noviello, referring to the $850, later commented to the supervisor, "that was a nice envelope for starters." After contacting authorities, the supervisor conducted a controlled purchase from Noviello during which the defendant distributed approximately 3.7 grams of cocaine for $200. (Source)

USPS Employee Sentenced To Prison For Stealing Nearly $400,000 In Federal Tax Refund Checks From The Mail - October 24, 2022

Kevin Streeter was employed by the U.S. Postal Service at a mail processing center in Sarasota, Florida.

He exploited his position by stealing approximately 40 federal tax refund checks from the U.S. mail that were enroute to the intended taxpayers living in the Middle District of Florida. Streeter and others then sold or attempted to sell the checks to third parties. The tax refund checks, issued by the U.S. Department of Treasury, ranged in amounts from $4,000 to over $100,000, with an aggregate value of over $398,000. (Source)

USPS Mail Carrier Charged For Role In Cocaine Distribution - October 11, 2022

Nathasha Prieto, was a United States Postal Carrier, who provided addresses on her postal route to Angel Coss, who arranged for the shipment of packages containing kilograms of cocaine from Puerto Rico to those addresses.

Instead of delivering the packages, Prieto removed the packages from the mail stream so that the cocaine within them could be distributed by Coss. On August 15, 2022, the investigation resulted in the seizure, from Prieto, of packages shipped from Puerto Rico containing kilograms of cocaine. (Source)

Multiple USPS Employees And Others Arrested For $1.3 Million Fraud And Identity Theft Scheme - September 29, 2022

Between in or around December 2018, up to and including the present, members of the conspiracy worked with U.S. Postal Service mail carriers, to steal credit cards from the mail stream before those cards were delivered to the assigned credit card customers.

After obtaining the stolen credit cards, members of the conspiracy activated the cards using stolen personally identifiable information (PII) of the intended recipients. Members of the conspiracy then used the stolen cards to purchase luxury goods, including items manufactured by Chanel, Fendi, Hermes, and Dior, from high-end retailers, including major department stores. (Source)

3 USPS Employees And Others Arrested For $1.3 Million Fraud And Identity Theft Scheme - September 29, 2022

Between in or around December 2018, up to and including the present, members of the conspiracy worked with U.S. Postal Service mail carriers, including, among others, FABIOLA MOMPOINT, NATHANAEL FOUCAULT, and JOHNATHAN PERSAUD to steal credit cards from the mail stream before those cards were delivered to the assigned credit card customers.

After obtaining the stolen credit cards, members of the conspiracy activated the cards using stolen personally identifiable information (PII) of the intended recipients.

Members of the conspiracy, including RASHAAN RICHARDS, DEVON RICHARDS, CONRAD HERON, LOUIS JEUNE VERLY, and KAREEM SHEPHERD (Collectively The Shoppers), and others known and unknown, then used the stolen cards to purchase luxury goods—including items manufactured by, among others, Chanel, Fendi, Hermes, and Dior—from high-end retailers, including major department stores in, among other places, Manhattan, Brooklyn, and New Jersey.

Often, JOHNNY DAMUS, instructed the Shoppers to purchase particular luxury items in specific quantities. Working together with a close associate (CC-1), DAMUS functionally operated LuxurySnob.com, on which many of these fraudulently obtained luxury items were sold. LuxurySnob purports to be an "online consignment and personal shopping company" specializing in "pre-owned luxury items," but, in fact, many of the items it sells were purchased using stolen credit cards. (Source)

USPS Employee Admits To Role In Stealing $12,000 Worth Of Cell Phones From Mail / Then Selling - September 12, 2022

Nyasia Hutchinson was employed by the U.S. Postal Service as a postal service clerk at the Elizabeth Post Office (EPO).

From May 1, 2018, through Dec. 31, 2018, another EPO employee provided Hutchinson with 15 to 20 stolen cellphones that the employee had taken out of packages at the EPO that had been mailed to a Hillside, New Jersey, business. Hutchinson admitted that she taped up empty packages and placed them back in the mail stream after cellphones had been removed. Hutchinson later sold the stolen iPhones which had a total approximate value of $12,000, keeping the sales proceeds for herself. (Source)

USPS Mail Carrier Pleads Guilty To Stealing Hundreds Of Pieces Of Mail - August 9, 2022

Between December 2020 and May 2021, Umberto Pignataro, while employed as a Mail Carrier for the U.S. Postal Service, stole hundreds of pieces of mail, including packages and greeting cards that contained cash, gift cards and other items of value. During the investigation, video surveillance captured Pignataro rifling through, destroying and pocketing pieces of mail while servicing his mail route.

When confronted by investigators in May 2021, Pignataro admitted stealing mail, and also admitted that he possessed a firearm and used cocaine at work. He was then placed on unpaid leave. (Source)

USPS Mail Carrier Pleads Guilty To Her Role In $462,000 Mail Fraud Conspiracy - August 9, 2022

Jasmine-Royshell Kanisha Black pleaded guilty today to her role in a conspiracy to commit mail fraud in connection to the illegal possession of unemployment benefit debit cards issued by the Nevada Department of Employment, Training and Rehabilitation (DETR) and Arizona's Department of Economic Security (DES). These agencies administer Nevada's and Arizona's unemployment insurance program, respectively.

Black who was employed as a U.S. Postal Service Mail Carrier, assisted co-conspirator Vincent Okoye to fraudulently obtain unemployment insurance benefits from DETR and DES using other people's personal identifying information, without their consent. Black used her position to help Okoye find either vacant residences or rarely-checked mailboxes to which fraudulently obtained debit cards could be sent. Black then intercepted and delivered those cards to Okoye in person. In total, DETR and DES approved of at least $462,000 in benefits for these fraudulent claims submitted by Black and Okoye. (Source)

USPS Mail Carrier Pleads Guilty To Role In Scheme To Deliver Drugs Through Mail In Exchange For Bribes - August 5, 2002

In 2014, Elliott Sheppard worked as a U.S Postal Service (USPS) mail carrier.

In exchange for bribes, he used his position to deliver five-pound packages of drugs through the U.S. mails to Dexter Frazier, a local drug trafficker who sold cocaine and marijuana.

In 2016, Frazier approached Sheppard about delivering additional drug packages. Sheppard was on disability leave from the USPS at that time and unable to intercept and deliver packages. So Sheppard offered to recruit other mail carriers to deliver drugs for Frazier, if Frazier paid Sheppard referral fees consisting of a mix of cash and marijuana. Frazier agreed.

Sheppard then contacted two coworkers, Tonie Harris and Clifton Lee. Sheppard explained to Harris and Lee that in exchange for payment, Frazier needed them to deliver packages of drugs.

Sheppard instructed Harris and Lee how to arrange the deliveries to avoid detection. Harris and Lee agreed to participate in the scheme after which Sheppard gave their phone numbers to Frazier. Frazier then coordinated the illegal deliveries with Harris and Lee. Harris and Lee each delivered three packages for Frazier believing they contained two kilograms of cocaine or 10 pounds of marijuana. (Source)

USPS Union President Gets Probation For Embezzling $80,000+ Of Union Funds For Personal Use: Meals, Fuel, Transportation, Shopping & Travel - June 28, 2022

Scott Rodgers embezzled a total of $80,756.

From 2016, when he became president of Postal Mail Handlers Local 314, to April 2020, Rodgers made four unauthorized ATM withdrawals from the union account and used the union debit card for personal purchases including meals, fuel, transportation, shopping and travel. He also falsely claimed and received "lost time" payments, or compensation for wages lost when performing work for the union. (Source)

USPS Mail Carrier Arrested For Scheme To Steal $800,000 In Unemployment Insurance Debit Cards - May 26, 2022

From August 2020 to February 2021, Stephen Glover and McKenzie fraudulently obtained debit cards issued by the California Employment Development Department (EDD), which administers the state's unemployment insurance program. The debit cards were issued based on applications for pandemic-related unemployment benefits submitted using approximately 50 stolen identities and containing false statements claiming COVID-related job losses, the affidavit states. The EDD debit cards were issued in the names of victims, some of whom had never resided in, worked in, or even visited California. Glover and McKenzie allegedly split the cash withdrawn using the EDD debit cards, some of which had balances exceeding $30,000.

The scheme allegedly involved more than 50 fraudulent claims to EDD, which resulted in EDD issuing cards that had approximately $798,733 in funds in those names, of which at least $318,771 has been withdrawn from the debit cards. (Source)

USPS Employee & Son Charged With Conspiracy Involving Stolen Postal Money Orders Worth $5 Million+ - May 23, 2022

Dewayne Morris Sr., was a supervisor for post offices in Venice, Playa Del Rey, and Marina Del Rey. He ordered and received 10,000 blank Postal money order forms. A subsequent audit revealed that approximately 5,100 of those 10,000 money order forms were missing. With a maximum value of $1,000 per money order, the potential value of the missing money order forms is $5.1 million.

Morris Jr., distributed the missing money orders to co-conspirators. The money orders Morris Jr. distributed to co-conspirators were materially altered to appear as if they had been paid for and lawfully issued by a post office, when in fact they had not. Morris Jr. also provided co-conspirators with counterfeit driver's licenses bearing fictious identities. The co-conspirators used those counterfeit documents to open checking and savings accounts at financial institutions throughout the country, deposited the stolen money orders into the accounts, and withdrew the cash proceeds before the financial institutions detected the fraud. (Source)

USPS Employee Pleads Guilty To Accepting $6,500+ Of Illegal Gratuities And Free Construction Work From A USPS Contractor - May 4, 2022

Thomas Berlucchi , is a Facilities Engineer for the United States Postal Service (USPS).

Berlucchi stands convicted of accepting illegal gratuities from Michael Rymar, who was the owner of a Rochester Hills company, Horizons Materials & Management LLC, which was awarded contracts to repair USPS buildings in Michigan and New York.

From 2015 to 2018, Berlucchi and other USPS engineers awarded Rymar's company over $5 million in contracts.

Berlucchi admitted that between 2013 and 2018, he had accepted over $6,500 in illegal gratuities from Rymar because Rymar sought to continue to receive USPS work from Berlucchi. Berlucchi admitted accepting free construction work on his cottage (including exterior stairs and a new roof), free hotel rooms, and donations by Rymar to Berlucchi's preferred organization. (Source)

USPS Contractor Charged For Stealing $1.2 Million+ From Contract To Repair USPS Building - March 25, 2021

Michael Rymar is charged with embezzling government funds from the United States Postal Service (USPS).

From 2015 to 2018, USPS engineers awarded Rymar's company, Horizons Materials & Management LLC, with over $5 million in contracts for repairs on USPS buildings in Michigan and New York. But the documentation Rymar provided contained false and fraudulent statements, oftentimes dramatically and falsely overstating the amount he paid subcontractors to complete the repairs. Rymar also falsely inflated the amount he paid his own employees and the cost of materials on USPS jobs. Over the course of the three-plus year fraudulent scheme, Rymar stole over $1.2 million from USPS out of the $5 million in contracts he was awarded. (Source)

USPS Post Office Manager & 2 Co-Conspirators Charged In Conspiracy Involving Theft Of $1.7 Million In Checks From Mail - March 9, 2022

James Lancaster was the former Manager of Customer Service at the Indianapolis' New Augusta Post Office. He has been charged with conspiracy to commit bank fraud and theft of mail.

Lavaris Yarbrough and Jordan McPhearson were charged with bank fraud and conspiring with Lancaster to commit bank fraud.

Between May 11, 2020, and June 23, 2021, Lancaster stole checks from the mail. Lancaster gave the stolen checks to McPhearson, sometimes receiving cash in exchange. McPhearson fraudulently negotiate the stolen checks, depositing them into an account belonging to someone other than the intended payee. Occasionally, McPhearson provide stolen checks to Yarbrough who fraudulently negotiate them.

Throughout the course of the conspiracy, Lancaster stole more than 270 pieces of U.S. mail from the New August Post Office. This mail contained checks from more than 50 different local businesses. In total, the value of the stolen checks was around $1.7 million. (Source)

USPS Contract Employee Pleads Guilty To Possession Of Stolen Mail With Intent To Steal Money - March 2, 2022

Miranda Farleigh pleaded guilty to possessing stolen mail. Farleigh faces a maximum penalty of five years in federal prison. A sentencing date has not yet been set. Farleigh had been indicted on February 1, 2022.

Farleigh worked as a contract employee of the United States Postal Service delivering mail for the Lady Lake Post Office. Farleigh's route included mail delivery services to postal stations in The Villages. On or about November 23, 2021, Farleigh's supervisor discovered several tubs and bags of U.S. Mail in Farleigh's possession that had been rifled (Unlawfully Opened). When confronted, Farleigh admitted to law enforcement that she had been opening outgoing mail in Lake and Sumter Counties for a month with the intent to steal money and gift cards to support her heroin addiction. In total, approximately 4,000 pieces of mail had been rifled through by Farleigh. (Source)

USPS Employee Sentenced To Prison For Stealing $232,000+ Of Bank Checks & Credit Cards From Mail - February 18, 2022

Johnson Ogunlana was a letter carrier for the U.S. Postal Service (USPS).

Between July 25, 2016 and February 5, 2019, Ogunlana, and his co-conspirator Samson Oguntuyi, conspired with others to steal bank checks and credit and debit cards from the mail, open fraudulent business banking accounts using the names of victim businesses and the stolen identities of victim postal customers to negotiate the stolen checks by depositing them into the fraudulent bank accounts, and then conduct transactions with stolen payment cards and with money derived from the stolen checks.

Ogunlana has been ordered to pay $232,588 in restitution. (Source)

U.S. Postal Service Employees Involved In Stealing Mail As Part of Bank Fraud Scheme - February 14, 2022

From February 2019 to May 2020, Jeffrey Bennett conspired to fraudulently obtain money from victim financial institutions by depositing counterfeit checks and checks stolen from the mail into accounts at these financial institutions and withdrawing funds before the financial institutions identified the fraudulent checks and blocked further withdrawals.

Bennett and his conspirators arranged for U.S. Postal Service (USPS) employees to steal credit cards and blank check books from the mail in exchange for cash payments. USPS employees provided the checks to Bennett and his conspirators, who forged the signatures of the accountholders and negotiated the checks by making them payable to individuals, some of whom were New Jersey high school students, who had given Bennett and his conspirators access to their accounts, also in exchange for cash. Bennett and his conspirators obtained and attempted to obtain approximately $366,000 from victim financial institutions. (Source)

USPS Employee Pleads Guilty To Stealing Government Property (Tires) And Selling For Personal Gain - December 15, 2021

Teddy Hale is a former employee of the United States Postal Service who worked at the vehicle maintenance facility.

Hale admitted that from June 15, 2017 and continuing through September 28, 2018, he stole more than 71 vehicle tires from the vehicle maintenance facility. Hale hid his thefts by using his position of employment to manipulate tire inventory. After Hale stole the tires, he sold them for his personal financial benefit. (Source)

USPS Employee Sentenced To Prison For Stealing Over 60 Pieces Of Mail With Checks Totaling $650,000 - Dcember13, 2021

Amy Jurisic worked as a postal clerk for the Dubuque Post Office in 2017 and 2018. Starting in June 2017 and lasting through at least October 2018, Jurisic stole over 60 pieces of mail.

Jurisic specifically stole mail that contained checks made out to a business located in Dubuque. Evidence showed that she then gave the checks to an individual in Chicago who was part of a check-cashing operation. The operation would change the names on the check and attempt to deposit the checks into various bank accounts. Overall, Jurisic stole nearly $650,000 in checks. Of that amount, approximately $62,000 was actually deposited into bank accounts. Other checks were flagged as fraudulent and banks did not process the deposits. (Source)

USPS Employee Pleads Guilty To Stealing $29,000+ From USPS For Personal Use - December 13, 2021
Tranese Mitchel was formerly employed as a lead sales and service clerk with the USPS in Houston.

She admitted she issued fraudulent refunds by creating no-fee postal money orders. She then cashed against her drawer at the post office where she worked. Mitchell fraudulently issued and cashed a total of $29,947.30. She admitted using the money for her own benefit. (Source)

USPS Clerk Sentenced To Prison For Stealing Mail & Passport Applications To Commit Bank Fraud - December 7, 2021
Jasmine Wynne was a Postal Clerk with the United States Postal Service (USPS) at the St. Petersburg Florida Retail Post Office location. She conspired with others to defraud federally insured financial institutions. Wynne opened First-Class mail and photographed personal identifying information (PII) and bank account information. Wynne then forwarded the photographs to co-conspirators for use in a bank fraud scheme. Wynne also photographed United States Passport applications that were processed at her post office location to gain applicants' PII and bank account information. She then forwarded that information to co-conspirators.

Wynne also stole restricted postal arrow keys, whhich are special master keys that open USPS collection boxes, banks of mailboxes at apartment complexes, and any other mailbox keyed with an arrow lock. Wynne then provided the postal arrow keys to co-conspirators for use in the charged conspiracy. (Source)

USPS Employee Pleads Guilty To Stealing $4,800+ From Mail - November 17, 2021
From August 2018 to October 2020, Colleen McAvoy was a part-time letter carrier for the USPS in Washington County, New York, based at the Cambridge Post Office.

In pleading guilty, she admitted to opening mailed packages in order to steal U.S. currency, gift cards and lottery tickets contained inside of those packages. She admitted to stealing items worth a total of approximately $4,889.25. (Source)

USPS Contractor Employees Charged Following Seizure of 8,000+ Pieces of Stolen Mail Worth $4 Million+ - November 2, 2021
Two Lubbock postal contractors have been charged with possession of stolen mail. The investigation which culminated in the recovery of more than 8,000 pieces of mail worth more than $4 million, marks the largest ever seizure of stolen mail in Northern District of Texas history.

Joe Rivas and Jessica Solomon were former co-workers at Cargo Force, Inc., a company that contracts with the United States Postal Service to load mail into and out of air containers destined for flights to and from the Lubbock International Airport.

During their shifts, Rivas and Solomon allegedly sifted through mail looking for items containing cash, gift cards, checks, and money orders. They allegedly stole that mail and stashed it in 55gallon trash bags at their residences. Among the checks they stole were a $25,728 check made payable to a telecom co-op, a $15,000 check to a consulting group, and a $241,1863 check to a facilities management and food services company. (Source)

USPS Employee Pleads Guilty To Stealing Cash And 44 Gift Cards From Letters - November 1, 2021
Nathaniel Bonilla was a mail processing clerk at the U.S. Postal Service's Process and Distribution Center (PDC) in Hartford. Between April 2020 and October 2020, Bonilla opened mail envelopes with a razor blade and removed cash and dozens of gift cards or prepaid debit cards for his own personal use.

In September 2020, a woman in New York mailed a letter containing a $500 Home Depot gift card to a family member in Torrington. The Torrington resident received the envelope, but it had been opened and the gift card had been removed. Bonilla was subsequently captured on Home Depot in-store surveillance footage using the gift card to buy merchandise.

On October 16, 2020, investigators confronted Bonilla as he was opening a letter with a razor blade. On that date, a search of his personal bag contained 44 gift cards that he had previously stolen while at work, and 37 opened envelopes at his workstation at the Hartford PDC. (Source)

7 Former USPS Employees Charged With Stealing Credit Cards From Mail - September 29, 2021
The indictments alleges that credit cards and other financial instruments were stolen from the mail and provided to others in exchange for cash or other items.

Some of the defendants unlawfully obtained USPS customers' personal identifying information, including dates of birth and Social Security numbers, which was then used to fraudulently activate the stolen cards, the charges allege. The newly charged USPS employees delivered mail in Chicago or processed and sorted the mail at a USPS facility in suburban Palatine. (Source)

USPS Employee Admits To Stealing Credit Cards From Mail Which Resulted In $2,000+ Of Fraudulent Charges On Customers Credit Cards - September 23, 2021
From April 1 to July 23, 2019, Myriam Jimenez a postal service employee.

Jimenez admitted to stealing credit cards addressed to third-party victims and mailed to addresses on postal routes in Elizabeth and Roselle Park, New Jersey, that she provided to other individuals in exchange for offers of $100 per card. The fraudulent charges on the credit cards Jimenez stole totaled over $2,000. (Source)

USPS Employee Admits Stealing $35,000 Worth Of Cell Phones From Mail - September 16, 2021
Kyle Terry was employed by the U.S. Postal Service as a mail handle assistant at a national postal distribution center in Jersey City.

From Nov. 1, 2017, to Jan. 28, 2018, Terry stole 39 cell phones having a total approximate value of $35,000 from mail that passed through that distribution center. (Source)

USPS Employee Admits Stealing Credit Cards From Mail Resulting In $100,000 Loses To Victims - August 24, 2021
Kyle Williams was employed by the USPS.

From July 2019 to August 2020, Williams stole from the mail credit cards issued by financial institutions and provided those credit cards to his conspirators, who fraudulently activated them and used them to make and attempt to make purchases without the cardholders' authorization, including buying gift cards and electronics.

The victims have incurred over approximately $100,000 in intended and actual losses from fraudulent purchases made using their stolen credit cards.

In addition to stealing and illegally using credit cards, Williams and his conspirators also schemed to fraudulently use over $11,000 of funds pre-loaded onto Economic Impact Payment (EIP) cards issued by the U.S. Department of Treasury and sent in the U.S. mail pursuant to the Coronavirus Aid Relief Economic Security Act (CARES Act), that were stolen from the mail. (Source)

USPS Mail Carrier Sentenced To Prison For Dumping 5,800+ Pieces Of Mail In Woods - August 4, 2021
Runner Up For Insider Threat Of The Year - Not Sure There Where Any Behavioral Indicators

Tanner Brown admitted that between January 1, 2019, and July 24, 2019, while working as a postal carrier for the United States Postal Service, he intentionally detained and failed to deliver 5,833 pieces of mail.

Instead of delivering this mail to its intended recipients in Onondaga County, Brown drove it to Sharon Springs, New York, where he dumped some of it in a grassy field and the rest of it in a wooded area underneath a pile of discarded tires. When agents recovered the mail from those locations, they discovered that much of it was First-Class Mailand that most of it was wet, dirty, and/or covered in bugs. The Postal Service eventually delivered as much of the recovered mail as it could, and Brown is no longer employed by the Postal Service. (Source)

USPS Employee Charged With Stealing $4,000+ Including iPad, SmartWatch, Reebok Shoes, Etc. From Mail - June 21, 2021
Btween July and September of 2020, Sa'Shanna Estell a United States Postal Services mail processing associate, knowingly removed from and stole from the mail a $3,870 cashier's check, 8 gift cards totaling approximately $330, an Apple iPad, a smartwatch, a pair of Reebok shoes, other clothing, two packages of THC edibles and $76 in cash.

In total, Estell is estimated to have stolen $4,594.67. (Source)

USPS Employee Pleads Guilty To Sealing Over $90,000 In Cash And Stamps From The USPS - June 15, 2021
Between October 2017 and June 2018, Lisa Mesler while employed by the USPS as a Station Manager, stole $63,265.96 from the cash register drawers of sales associates, which she supervised. Mesler stole money on 53 different occasions. Also, on multiple occasions during that time period, the defendant stole stamps. The value of the stamps stolen was $28,265.30. (Source)

USPS Mail Carrier Admits Dumping Mail, Including Election Ballots Sent To New Jersey Residents - May 27, 2021
A USPS Mail Carrier (Nicholas Beauchene) admitted that on Sept. 28, Oct. 1, and Oct. 2, 2020, he discarded into dumpsters in North Arlington, New Jersey, and West Orange 1,875 pieces of mail that he was assigned to deliver to postal customers in West Orange and Orange, New Jersey.

This mail included 627 pieces of first-class mail, 873 pieces of standard class mail, two pieces of certified mail, 99 general election ballots destined for residents in West Orange, and 276 campaign flyers from local candidates for West Orange Town Council and Board of Education. Law enforcement recovered the mail on Oct. 2, 2020, and Oct. 5, 2020, and placed it back into the mail stream for delivery. (Source)

USPS Employee Pleads Guilty To Stealing Medication Intended For Veterans - March 1, 2021

Ammie Hale a USPS employee pleaded guilty to stealing mail on February 26, 2020, July 1, 2020, and August 5, 2020.

According to court documents, from September 2019 through July 2020, the United States Postal Inspection Service- Office of the Inspector General (USPIS-OIG) received over 40 reports from the Salem, Virginia Veterans Affairs Medical Center of medication parcels mailed to veterans in the Tazewell, Virginia area that were never delivered.

Agents of the USPS-OIG reviewed available video footage and observed Ammie Hale on two different occasions, while working at the Tazwell Post Office, removing parcels from the sorting area, and taking them to an area of the Post Office where employees keep personal belongings and hiding the parcels in her purse. On August 5, 2020, agents conducted on-site surveillance and caught Hale stealing pills from a package addressed from the Veterans Affairs Medical Center. Hale was interviewed on August 5 and falsely told investigators that she had never stolen mail prior to that day. (Source)

USPS Mail Carriers Among 11 Individuals Charged In Conspiracy To Steal Credit Cards From the Mail - February 26, 2021

Law enforcement uncovered the 18-month conspiracy through a federal investigation dubbed Operation Cash on Delivery.

The former USPS employees, who at the time worked as mail carriers in the Chicago area, stole credit cards and other financial instruments from the mail and provided them to others in exchange for cash or other items. Two of the defendants unlawfully obtained USPS customers' personal identifying information, including dates of birth and Social Security numbers, which was then used to fraudulently activate the stolen cards and make purchases at various retailers, including Best Buy, Fry's Electronics, Walmart, and Meijer, the charges allege. (Source)

USPS Mail Carrier Pleads Guilty To Failing To Deliver Over 700 Pieces Of Mail Which Included Three Absentee Ballots - January 4, 2020

On November 3, 2020, Customs and Border Protection (CBP) Officers encountered the defendant, an employee of the United States Postal Service (USPS) at the time, at the Peace Bridge Port of Entry.

In the trunk of Brandon Wilson's vehicle, officers found 701 mailings, and a USPS employee uniform and employee identification badge. The mailings included three (3) official absentee ballots mailed from the Board of Elections to voters, 218 first class mailings, 106 political mailings, 36 regular nonprofit mailings, 305 regular standard mailings, and 33 magazine / catalogue mailings. (Source)

USPS Employee Charged For $230,000+ Fraud, Embezzlement Scheme Over 7 Years - November 18, 2020

ILiganoa Laufo illegally collected more than $230,000 over the course of a fraud scheme that began in 2011 and continued until 2018.

Laufo lied about her household composition and income, used stolen identities to claim additional benefits and open bank and credit accounts, and stole checks from the mail during a period when she was employed by the U.S. Postal Service.

Between April 2011 and December 2018, Laufo applied for welfare benefits, including food and income assistance, by claiming her husband did not live with the family. She submitted falsified documents to bolster the claim that her husband lived elsewhere. Had her husband's income been counted, she would not have qualified for the assistance she received.

Laufo also stole and misused the identity information of minor children who lived in American Samoa, claiming they resided with her when they did not. By claiming these children, she received additional food and childcare benefits. LAUOFO submitted forged letters from doctors and landlords to support her claim that the children resided with her.

Starting in 2015, Laufo used the identity information of two family members residing in California and an acquaintance in American Samoa to receive additional benefits including food assistance, cash assistance, and childcare funds. She claimed still more children—again, actually living in American Samoa—were residing with her under these three false identities and created letters and documents to bolster those claims as well. Laufo received more than $220,000 from this scheme to which she was not entitled.

Laufo used the identities she stole to open bank and credit accounts. She opened one of those accounts in the name of her ex-husband three years after he died. She deposited worthless checks in the bank account and quickly withdrew cash before the bank realized the fraud. More than $10,000 in loss resulted from that conduct.

In March 2018, when Laufo was employed by the U.S. Postal Service as a letter carrier, she stole and deposited two checks from the mail she was assigned to deliver. She deposited the checks into an account in the name of one of the identities she had stolen in the benefits fraud scheme. (Source)

USPS Employee Sentenced To Prison For Stealing 400+ Mobile Phones Out of Packages In The Mail / Selling For Profit - October 14, 2020

Beginning in about August, 2019, Rico Alvarez, an employee of the United States Postal Service, began stealing smartphones placed into the mail for delivery to customers. Over the course of the next three months, Alvarez stole more than 400 phones, by surreptitiously opening the box as it passed his mail sorting station, removing the phone, and then sending the empty package on for delivery to the intended recipient.

On the day he was caught by OIG Special Agents, he had over a dozen stolen phones in his possession. When interviewed, Alvarez admitted to stealing high end, recently released, smartphones, which he subsequently sold for his own profit. (Source)

USPS Employee Sentenced To Prison For Stealing Nearly $40,000 In Postal Money Orders - September 9, 2020

Between July 2017 and December 2018, Keith Sanford was employed by the U.S. Postal Service and worked on a rotating basis at the Granby, West Granby and East Hartland Post Offices.

Between April and December 2018, Sanford issued 139 postal money orders totaling $39,937.02 to himself and, in certain instances, his associates, without remitting payment for them. Sanford received all of the proceeds from this scheme. The judge ordered Sanford to pay full restitution. (Source)

USPS Postmaster Sentenced To Prison For Stealing $7,000 In Government Funds - June 2, 2020

Adam Lavertue began working the USPS in April 2008 and became Postmaster of the Groton Post Office in June 2015. Lavertue performed a variety of managerial and administrative tasks to facilitate the daily operations of the Post Office, including maintaining the facility's operational functions, handling customer transactions and managing mail clerks and delivery staff.

In February 2017, Lavertue began using the purchase charge card issued to the Groton Post Office to make over $500 in personal purchases, including food, beverages and tobacco products. Additionally, Lavertue used Post Office Voyager cards, which are used by USPS mail couriers to fuel the official USPS delivery vehicles, to fuel his personally owned vehicle, charging over $5,000 in fuel. Lavertue also stole over $1,000 in cash from his assigned cash register drawer and reserve at the Groton Post Office. Lavertue's scheme cost the USPS approximately $7,000. (Source)

USPS Employee Sentenced To Prison For Stealing More Than $50,000 Worth Of Mail - April 17, 2020

John R. Elbayeh of Albany, was sentenced today to time served for stealing Apple iPhones, gold coins, small gold bars and other valuable items from mailed packages while employed as a postal clerk.

Elbayeh worked as a lead mail processing clerk at the USPS Processing and Distribution Center in Albany, from December 2012 through December 2018. He admitted that for approximately 2 years ending in December 2018, he stole valuable items from the mail, including iPhones and gold coins, which he pawned for a total of $50,362.22.

Shortly after being interviewed by federal agents in December 2018, Elbayeh took a one-way flight to Beirut, Lebanon, and remained outside the United States until October 17, 2019. On that date, USPS-OIG Agents arrested him at Dulles International Airport in Virginia, where Elbayeh had just arrived from a flight originating in Cairo, Egypt. Elbayeh had been in custody since that time. (Source)

USPS Mail Carrier Addicted To Opioids Sentenced To Probation For Stealing 147 Medication Parcels For His Own Personal Use - March 11, 2020

Aaron Hine was sentenced to a five year term of probation and six months home confinement for stealing prescription medicine from the United States Mail.

According to court records, Hiner was an employee of the United States Postal Service and assigned to the St. Louis Metro Annex in Hazelwood, Missouri between 2004 and March 2019. On January 15 and March 5, 2019, Hiner stole 147 Express Scripts medication parcels from the mail. Hiner pled guilty and admitted that, because of his addiction to opioids, he stole the Express Scripts parcel mailings. The estimated loss associated with his theft is $35,742.57. (Source)

USPS Clerk Sentenced To Prison For Embezzling $3,000 Over 2 Years - March 6, 2020

James Barnes was the lead Sales and Service Associate at the Midwest City Branch Post Office when he conducted a scheme to steal postal funds by taking cash for stamps without properly accounting for the sales. He was charged with one count of embezzlement of postal funds in excess of $1,000, one count of theft of government money in excess of $1,000, and four counts of making false entries in the U.S. Postal Service's records.

On July 11, 2019, a jury convicted Barnes on those six counts. The jury heard that Barnes made false record entries into his cash register at least 178 times from October 2015 through June 2018 and took almost $3,000 belonging to the U.S. Postal Service. (Source)

3 USPS Employees Admit To Roles In Bank Fraud Scheme To Steal $75,000+ In Checks - February 11, 2020

Nicole Georges pleaded guilty in court to information charging her with theft of mail and conspiracy to commit bank fraud. Raheem Moore and Daquan Pruitt previously pleaded guilty to separate informations charging each with conspiracy to commit bank fraud, as a result of the scheme to cash the stolen checks.

Georges stole checks from the USPS station in Chester, New Jersey where she was employed. Georges and her conspirators then fraudulently deposited them into various bank accounts, and withdrew the money, often that same day or a day later before the checks were reported stolen. The stolen checks had a total value of over $75,000. (Source)

Federal Authorities Charge 33 People With Crimes Against The USPS, Most Were USPS Employees - August 26, 2016

33 defendants were charged as part of a sweep targeting criminal activity that has victimized the United States Postal Service (USPS) and its customers. Most of the defendants charged as part of the sweep are USPS employees who allegedly stole mail, embezzled from the agency or, in one case, failed to deliver nearly 50,000 pieces of mail.

The 33 defendants are charged across 28 cases, about half of which allege mail theft and/or possession of stolen mail by USPS employees and contractors. Other cases charge USPS employees with conspiracy, embezzlement, bank fraud, and false statements. Five of the cases allege crimes by non-employees, including mail theft and fraud related to the use of credit cards that had been stolen from the mail. (Source)

U.S. STATE DEPARTMENT

State Department Government Contractor Arrested On Espionage Charges To Aid Foreign Government - September 21, 2023

Abraham Lemma is a naturalized U.S. citizen of Ethiopian descent.

Limma was charged with gathering or delivering national defense information to aid a foreign government; conspiracy to gather or deliver national defense information to aid a foreign government; and having unauthorized possession of national defense information and willfully retaining it.

Lemma worked as an IT administrator for the Department of State, and as a Management Analyst for the Department of Justice. In those positions, Lemma was granted a TOP SECRET security clearance and granted access to classified systems.

Between December 19, 2022, and August 7, 2023, Lemma copied classified information from Intelligence Reports and deleted the classification markings from them. Lemma then removed the information, which was classified as SECRET and TOP SECRET, from secure facilities at the Department of State against protocol.

Lemma used an encrypted application to transmit classified national defense information to a foreign government official associated with a foreign country's intelligence service. In these communications, Lemma expressed an interest and willingness to assist the foreign government official by providing information. In one communication, the foreign official stated, "It's time to continue your support." Lemma responded, "Roger that!" In other chats, the foreign official tasked Lemma to focus on information related to particular subjects, and Lemma responded "absolutely, I have been focusing on that all this week." The classified national defense information Lemma transferred to the foreign official included satellite imagery and other information regarding military activities in the foreign country and region. (Source)

State Department Employee Sentenced To Prison For Providing Confidential Bidding Information To Bidder And Received $60,000 Kickback Payments in Return - April 8, 2022
May Salehi was a former State Department employee.

Salehi was involved in evaluating bids for critical overseas government construction projects such as U.S. embassies and consulates. Salehi gave confidential inside bidding information to a government contractor, and received $60,000 in kickback payments in return. (Source)

State Department Employee And Wife Sentenced To Prison For Trafficking In Counterfeit Goods From U.S. Embassy - March 18, 2021
Gene Thompson (Former U.S. Department of State Employee) and his spouse Becky Zhang, were sentenced for their roles in a conspiracy to traffic hundreds of thousands of dollars in counterfeit goods through e-commerce accounts operated from State Department computers at the U.S. Embassy in Seoul, Republic of Korea.

Thompson was an Information Programs Officer employed by the Department of State at the U.S. Embassy in Seoul, Republic of Korea, a position that required him to maintain a security clearance.

Zhang resided with him in Seoul. Between September 2017 and December 2019, Thompson Jr. and Zhang sold counterfeit goods on a variety of e-commerce platforms.

Thompson Jr. used his State Department computer at the embassy to create numerous e-commerce accounts, including additional accounts under aliases to continue the conspiracy and avoid detection after several e-commerce platforms suspended the couple's other accounts for fraudulent activity. Zhang took primary responsibility for operating the accounts, communicating with customers, and procuring merchandise to be stored in the District of Oregon. Thompson Jr. and Zhang also directed a co-conspirator in the District of Oregon to ship items to purchasers across the United States. (Source)

State Department Contracting Officer Sentenced To Prison For Accepting $520,000+ In Bribes For Procurement Fraud Scheme - February 14, 2020
A contracting officer (Zaldy Sabino) with the U.S. Department of State was sentenced today to 87 months of imprisonment followed by three years of supervised release after he was convicted of 13 counts of conspiracy, bribery, honest services wire fraud and making false statements.

Between November 2012 and early 2017, Sabino and the owner of a Turkish construction firm engaged in a bribery and procurement fraud scheme in which Sabino received at least $521,862.93 in cash payments from the Turkish owner while Sabino supervised multi-million dollar construction contracts awarded to the Turkish owner's business partners and while Sabino made over a half million dollars in structured cash deposits into his personal bank accounts. Sabino concealed his unlawful relationship by, among other things, making false statements on financial disclosure forms and during his background reinvestigation. (Source)

State Department Employee Sentenced To Prison For Embezzling 150,000+ From Department Of Defense - December 1, 2021
From 2015 through August 2018, Roudy Pierre-Louis was an employee of the State Department (SD) who worked at the Embassy of Haiti as the sole budget analyst for the Security Coordination Office (SCO).

In this role, Pierre-Louis was responsible for managing all lines of accounting for the SD and Department of Defense (DoD) associated with the SCO, which included per diem cash advances for individuals travelling to United States Southern Command events. Pierre-Louis also was designated as the SCO's Occasional Money Holder, allowing him to receive cash on behalf of other individuals who did not have full access to the Embassy in order to obtain cash advances for travel expenses, including, but not limited to, per diem, lodging, and air fare.

The Embassy maintained a vault, or cash cage, from which cash advances could be disbursed to employees providing documentation of supervisory approval. This cash cage was reconciled on a daily basis, as cash on hand along with approved disbursements were required to be reconciled and approved by a financial officer with the SD in order to balance and replenish the cash supply.

Pierre-Louis submitted fraudulent vouchers and supporting documents for cash advances in the names of Haitian Nationals that contained forged signatures of requesting and approving DoD supervisors. Unaware of this fraud, the Department of State released these cash funds to Pierre-Louis, which were subsequently reimbursed by the Department of Defense. During the relevant time period, from 2015 to August 2018, Pierre-Louis embezzled at least $156,950 from his wire fraud scheme. (Source)

U.S. GOVERNMENT LAW ENFORCEMENT AGENCIES

FEDERAL BUREAU OF INVESTIGATION

FBI Special Agent Convicted For Stealing From Citizens' Homes When Executing Search Warrants - September 23, 2024

From March 2022 to July 2023, Nicholas Williams stole money and property from multiple residences while executing search warrants in his official capacity.

Specifically, the plea agreement lists several instances in which Williams stole cash totaling nearly $10,000 as well as several silver bars which he had attempted to sell to another individual.

Williams proceeded to retain the money or property for his personal use. He used some of the money to purchase guns and related items.

In addition, Williams admitted to providing false statements with regard to several fraudulent charges on his government-issued credit card, making it appear they were case-related expenses, when they were not. He also took some legitimate FBI-purchased property and pawned for cash.

Since 2019, Williams worked as an FBI special agent in the Houston field office. He served on both the criminal violent gang and counterterrorism squads. (Source)

FBI Special Agent Sentenced To Prison For Conspiring To Violate U.S. Sanctions On Russia, Receiving $225,000 In Cash And Money Laundering - December 14, 2023

Charles McGonigal is a former FBI Special Agent in Charge of the New York Field Office.

From August 2017, and continuing through his retirement from the FBI in September 2018, McGonigal concealed from the FBI the nature of his relationship with a former foreign security officer (and businessperson who had ongoing business interests in foreign countries and before foreign governments. McGonigal received at least $225,000 in cash from the individual and traveled abroad with the individual and met with foreign nationals. The individual later served as an FBI source in a criminal investigation involving foreign political lobbying over which McGonigal had official supervisory responsibility.

McGonigal was sentenced to prison for conspiring to violate the International Emergency Economic Powers Act and to commit money laundering in connection with his 2021 agreement to provide services to Oleg Deripaska, a sanctioned Russian oligarch. (Source)

FBI Analyst Sentenced To Prison For Retaining 386 Classified Documents And Keeping Them At Her Home - June 21, 2023

Kendra Kingsbury is a former Intelligence Analyst with the Kansas City Division of the FBI, from 2004 to 2017. Kingsbury was assigned to a sequence of different FBI squads, each of which had a particular focus, such as illegal drug trafficking, violent crime, violent gangs, and counterintelligence. Kingsbury held a TOP SECRET//SCI security clearance and had access to national defense and classified information.

Kingsbury admitted that, over the course of her FBI employment, she repeatedly removed from the FBI and retained in her personal residence an abundance of sensitive government materials, including classified documents related to the national defense. In total, Kingsbury improperly removed and unlawfully and willfully retained approximately 386 classified documents in her personal residence. (Source)

FBI Special Agent Sentenced To Prison For Accepting $150,000 In Bribes Paid by Attorney Linked to Organized Crime Figure - February 27, 2023

Babak Broumand was an FBI special agent from January 1999 until shortly after search warrants were served on his home and businesses in 2018. He was responsible for national security investigations and was assigned to the FBI Field Office in San Francisco.

Broumand accepted $150,000 in cash bribes and other items of alue in exchange for providing sensitive law enforcement information to a corrupt lawyer with ties to Armenian organized crime.

From January 2015 to December 2018, Broumand accepted cash, checks, private jet flights, a Ducati motorcycle, hotel stays, escorts, meals, and other items of value from the organized crime linked lawyer.

In return for the bribe payments and other items of value, Broumand conducted law enforcement database inquiries and used those inquiries to help the lawyer and his associates avoid prosecution and law enforcement monitoring. (Source)

665 FBI Employees Left Agency After Misconduct Investigations According To Whistleblower Disclosure - October 6, 2022

Sen. Chuck Grassley (R-Iowa) said he obtained internal records from a whistleblower alleging 665 FBI employees retired or resigned following misconduct investigations to avoid receiving final disciplinary letters.

Grassley said the whistleblower provided an internal Justice Department report that indicated the employees left between 2004 and 2020 and included 45 senior-level employees.

“The allegations and records paint a disgraceful picture of abuse that women within the FBI have had to live with for many years,” Grassley wrote in a letter to FBI Director Christopher Wray and Attorney General Merrick Garland. “This abuse and misconduct is outrageous and beyond unacceptable,” Grassley continued.

Grassley’s office said Justice Department officials created the report following an Associated Press story in 2020 that revealed sexual conduct allegations among senior officials in the bureau.

The alleged report states the 665 employees left following "alleged misconduct," but it did not specify it as sexual misconduct, although the document is titled as such.

His office suggested the actual figure could be larger, because the data doesn't include departures that occurred during or just prior to the start of misconduct investigations.

The Associated Press investigation that apparently spawned the report's creation found that the bureau opted to transfer those facing accusations or allow them to retire.

"Congress has an obligation to perform an objective and independent review of the Justice Department's and FBI's failures and determine the accuracy of the data contained in the documents so that the American people know and understand what, if any, changes have been made to solve these significant problems," Grassley wrote in his letter. (Source)

FBI Special Agent Sentenced To Prison For Using $13,500 Of Government Funds For Blackjack Gambling In Las Vegas - August 17, 2022

From July 27 to July 31, 2017, Scott Carpenter while employed as a Special Agent with the FBI's New York City Field Office, he and 3 other FBI agents traveled to Las Vegas to conduct an undercover operation.

At the conclusion of the operation, Carpenter went to a casino's high limit room, where he gambled on blackjack with $13,500 belonging to the United States. (Source)

U.S. CUSTOMS & BORDER PROTECTION (CBP)

CBP Officer Sentenced To Prison For Receiving Bribes From Drug Cartel To Allow Drug-Laden Vehicles Into U.S. - October 28, 2024

During the trial, several witnesses testified that Leonard George agreed to allow drug-laden vehicles to enter the U.S. through his lane in late 2021. George would notify members of a drug trafficking organization when he was at work, what lane he was on, and that they had one hour to reach his lane. However, in February 2022, after an alert placed by law enforcement agents on a suspected drug smuggling vehicle was flagged entering George's Lane, George was forced to send the vehicle to secondary inspection, later revealing approximately 222 pounds of methamphetamine.

Undeterred, George allowed a second drug-laden vehicle affiliated with the drug trafficking organization and traveling directly behind the flagged vehicle to enter the U.S. with over 200 pounds of drugs. Text messages sent by George the following day reveal he received approximately $13,000 for the vehicle he allowed to enter the U.S. On the same day he received his bribe payment, George purchased a 2020 Cadillac CT5 for an associate of the drug trafficking organization as a gift. George delivered the Cadillac CT5 to the associate in Ensenada on Valentine's Day.

Over the course of six months, George continued to allow vehicles containing undocumented individuals to enter the U.S. through his lane. George repeatedly omitted passengers and the true names of drivers coming through his lane, instead entering the names of others to conceal his criminal activities. Law enforcement agents and prosecutors identified approximately 19 crossings associated with the criminal organizations during the six-month time period. Text messages confirmed George agreed to allow vehicles through his lane for $17,000 per vehicle, $34,000 for two vehicles, $51,000 for three vehicles, or $65,000 for four vehicles. One text message confirmed that George received $68,000 after he allowed four vehicles from one organization to enter his lane in June 2022.

Testimony from a witness confirmed that George purchased vehicles, motorcycles, and jewelry with the proceeds of his illicit activities. On George's days off, he travelled to Tijuana to visit Hong Kong Gentlemen's Club where he spent approximately $5,000 per trip. He would stand on the second level of the club and throw cash over the balcony to the dancers below, "showering" them with money. He would also buy bottles of alcohol, and occasionally gifts, for dancers. (Source)

CBP Employee Pleads Guilty To Stealing $67,000+ Worth Of Laptops And Attempting To Sell - October 22, 2024

On Dec. 13, 2023, Xavier Mittakarin removed the 27 laptops, valued at a total of over $67,000, from the facility, intending to sell them. On March 22, 2024, Mittakarin sold one of the laptops via eBay to a purchaser in California, who paid $2,803.26. On May 22 and May 27, Mittakarin sold eight more laptops via eBay to another purchaser in California, who paid a total of $16,706.76.

On Aug. 1, Mittakarin attempted to sell 18 laptops to another purchaser, who was actually an undercover officer, for approximately $28,000. Mittakarin brought the laptops to a prearranged meeting place and time, where he was arrested and the laptops were recovered from his vehicle. (Source)

CBP Officer Sentenced To Prison For Stealing $18,000+ In Cash From Airline Passengers - September 26, 2024

Between mid-2023 and early-2024, while working as a U.S. Customs and Border Protection (CBP) Officer at the Naples Airport in Florida, William Timothy stole approximately $18,700 in cash from airline passengers during 17 incidents of theft uncovered by CBP's Office of Professional Responsibility investigators.

Evidence collected during the investigation showed that Timothy was surreptitiously stealing cash from arriving international passengers during border enforcement examinations and currency verifications performed as part of his official duties as an assigned CBP Officer at Naples Airport. (Source)

Drug Cartel Bribed 2 CBP Agents To Let Drugs Into U.S. - September 5, 2024

2 CBP officers have been accused of working for a Mexican drug trafficking organization to allow vehicles loaded with fentanyl, heroin, cocaine, and methamphetamine to pass unchecked through their inspection lanes in southern California.

Prosecutors allege Jesse Garcia and Diego Bonillo "profited handsomely," earning tens of thousands of dollars for each drug-laden vehicle they ushered into the U.S. without scrutiny.

The indictment alleges that Garcia and Bonillo combined allowed more than 1,150 pounds of drugs into the U.S. on five occasions between April 2021 and February 2024. That total only accounts for the drugs that authorities later seized.

Their arrests came exactly a month before their former colleague, Leonard George, went on trial in a similar case. A federal jury convicted George in June of accepting hundreds of thousands of dollars in bribes in exchange for allowing smugglers to bring drugs and illegal immigrants through his inspection lane at the San Ysidro Port of Entry, just across the border from Tijuana. (Source)

CBP Agent Sentenced To Prison For Attempting To Distribute Methamphetamine & Receiving $100,000+ In Bribes - May 24, 2024

Former U.S. Customs Border Patrol Agent Hector Hernandez admitted that he took bribes to smuggle methamphetamine and people across the U.S.-Mexico border while on duty.

Hernandez acknowledged he took Mexico-based smugglers on a tour of the U.S.-Mexico border, showing them the best locations to sneak unauthorized immigrants into the U.S. He also provided information about the location of monitoring devices and cameras, information only known to him by virtue of his position as a Border Patrol agent. Hernandez admitted that he opened restricted border fences on several occasions to allow people to illegally enter the United States in exchange for cash payments of $5,000 per opening.

According to court records, Hernandez admitted that on May 9, 2023, he met with someone who unbeknownst to him was, in fact, an undercover federal agent, and agreed to pick up a bag full of narcotics that would be hidden near the border fence. Hernandez agreed to pick up the bag while on duty and deliver it to the undercover agent in exchange for $20,000.

Once the agreement was made, agents loaded the bag with 10 kilograms of fake methamphetamine, one pound of real methamphetamine, and a tracking device, before placing the bag in a storm drain near the border fence.

Later that evening, Hernandez drove his official vehicle to the storm drain while on duty and retrieved the bag. He drove the bag to his residence in Chula Vista and left the bag there for the remainder of his work shift. On May 10, 2023, after his shift was over, Hernandez returned home, retrieved the bag, and drove to meet with the undercover agent. Upon arrest, agents confirmed that that the bag still contained both the sham and real methamphetamine.

After Hernandez was arrested, agents searched his residence and found $131,717 in cash and 7.7 grams of cocaine. Hernandez admitted at least $110,000 of the cash represented proceeds he received in connection with his narcotics trafficking and bribery activities. (Source)

CBP Agent Sentenced To Prison For Accepting Bribes For Drug Smuggling - April 12, 2023

On August 9, 2020, while working as a United States Border Patrol Agent, Carlos Passapera drove his Border Patrol vehicle into the Arizona desert, and retrieved two large duffel bags. Passapera then changed vehicles and transported the duffel bags to the Phoenix Sky Harbor International Airport, where he parked and loaded the bags into the vehicle of a co-conspirator. The co-conspirator was stopped by law enforcement shortly after leaving the airport parking lot.

A search of the two duffel bags revealed multiple packages of cocaine, fentanyl, and heroin. Approximately 21 kilograms of cocaine, one kilogram of fentanyl, and one kilogram of heroin were seized. An additional $311,100 in U.S. currency was seized from Passapera's safe deposit box. Passapera admitted to accepting large cash payments in exchange for using his position to smuggle drugs. (Source)

CBP Agent Sentenced To Prison For Bribery, Firearms, Narcotics Charges - December 27, 2022

Between July and August 2018, Monreal-Rodriguez, a former U.S. Border Patrol (USBP) agent, was involved in two firearm-related conspiracies wherein he both unlawfully purchased firearms from federally licensed firearms dealers on behalf of other individuals and provided firearms to felons, who are prohibited from possessing firearms.

While the investigations into the firearms conspiracies were ongoing, Monreal-Rodriguez also conspired to import narcotics into the United States from Mexico, from January 8, 2018, until his arrest on September 25, 2018. During this time, a drug trafficking organization he worked with smuggled narcotics across the border. Monreal-Rodriguez would retrieve the narcotics and take them past the checkpoint several miles from the border, often in his USBP vehicle and then transport the drugs to the Tucson area. He admitted to distributing 116 kilograms of cocaine and 107 kilograms of marijuana as part of the conspiracy.

Additionally, Monreal-Rodriguez admitted to receiving cash proceeds from narcotics sales totaling at least $1.2 million, which he transported to the United States-Mexico border and then handed off to other individuals so the cash could be smuggled into Mexico. In exchange for his role in the narcotics conspiracy, Monreal-Rodriguez received cash payments. (Source)

CBP Officer Sentenced To Prison For Accepting $6,000 Bribe From Illegal Alien Who Was Convicted Felon - January 20, 2021

In early 2018, Jose Fuentes, then a CBP officer assigned to canine duty at the Nogales Port of Entry, agreed to allow an illegal alien into the United States in exchange for a $6,000 cash bribe.

Fuentes knew the alien was a convicted felon, and proposed that the alien enter the United States through the port of entry during Fuentes' shift. Surveillance footage shows Fuentes, on-duty and in uniform, pretending to swipe the alien's identification at the port of entry, and then waiving the alien through the pedestrian gate and into the United States. Fuentes later met up with the alien and another individual to receive the $6,000 cash bribe. (Source)

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)

3 Former DHS Employees Sentenced To Prison For Conspiracy To Steal Proprietary U.S. Government Software & Databases - January 26, 2024

3 former Department of Homeland Security (DHS) employees (Charles K. Edwards, Sonal Patel, Murali Venkata) were sentenced for a conspiracy to steal proprietary software and sensitive law-enforcement databases from the U.S. government for use in a commercial venture.

Edwards was the former Acting Inspector General of the DHS Office of Inspector General (DHS-OIG). Patel and Venkata were employed in DHS-OIG's information technology department. Edwards, Patel, and Venkata were all previously employed at the U.S. Postal Service Office of Inspector General (USPS-OIG).

Edwards, Patel, and Venkata conspired to steal proprietary U.S. software and databases containing sensitive law-enforcement information and the personally identifiable information (PII) of over 200,000 federal employees from DHS-OIG and USPS-OIG. They planned to use the stolen software and databases to create a commercial software product to be offered for sale to government agencies. As part of the scheme, the co-conspirators disclosed the stolen software and databases containing PII to software developers located in India. After Venkata learned of the investigation, he deleted incriminating text messages and other communications in an effort to obstruct the investigation. (Source)

Special Agent For U.S. Homeland Security Investigations Sentenced To Prison For Accepting $50,000 In Kickbacks From Informant - October 23, 2023

Anthony Sabaini was assigned to the Oakbrook Terrace, llinois field office of Homeland Security Investigations (HSI), a criminal investigative unit within DHS.

Evidence at trial revealed that Sabaini maintained a corrupt relationship with an HSI confidential informant and tipped off the informant to sensitive investigations conducted by other law enforcement agencies, including the FBI and DEA. In exchange for Sabaini's protection, the informant paid Sabaini at least $50,000. Sabaini also stole cash from drug dealers and pocketed money from HSI that had been earmarked for investigative activity.

Sabaini deposited more than $250,000 into a bank account for which he was the sole signatory. He made the deposits in more than 160 transactions, with the amount of each deposit being less than $10,000. The deposits were structured in an effort to evade federal reporting rules, which require financial institutions to notify the U.S. Department of the Treasury about transactions of more than $10,000. (Source)

The evidence also showed that Sabaini lied on official HSI memoranda in 2017 and 2018 to protect his corrupt relationship with the informant.

U.S. Homeland Security Investigations Agent Sentenced To Prison For Accepting $100,000 In Bribes From Person Associated With A Criminal Organization - November 21, 2022

Over an 18 month period that started in September 2015, Felix Cisneros accepted cash, checks, private jet travel, luxury hotel stays, meals and other items of value from a person who was associated with a criminal organization. Cisneros received approximately $100,000 in checks and gifts from Individual 1 in 2015 and 2016.

Cisneros accepted cash payments and other benefits to help an organized crime-linked person, including taking official action designed to help two foreign nationals gain entry into the United States. (Source)

U.S. DRUG ENFORCEMENT ADMINISTRATION (DEA)

DEA Employee Pleads Guilty To Embezzling $75,000+ - October 25, 2024

In September 2023, after 16 years of employment with the DEA, Scott Knox embezzled over $75,000 from a DEA vault to which he had access and control by virtue of his position as a Mission Support Specialist and Account Technician with the DEA in Phoenix.

In this role, his responsibilities included safeguarding the DEA Imprest Fund, which is a designated cash reserve for managing recurring DEA expenses, including operational funds utilized by agents in the field. Knox admitted that he deliberately stole $75,546 in cash from the Imprest Fund secure room. Knox attempted to conceal his actions from the DEA, but his embezzlement was uncovered during an internal audit the DEA conducted in March 2024. (Source)

DEA Task Force Officer Pleads Guilty To Conspiring To Distribute Narcotics - April 8, 2024

While employed as a Florida Highway Patrol Trooper and designated Task Force Officer with the Drug Enforcement Administration, Joshua Earrey and a co-conspirator engaged in widespread and extensive corrupt activity from 2017 - 2023. These corrupt acts included the theft of money and illegal drugs that were seized as evidence during criminal investigations; providing the illegal drugs to others to distribute on his behalf; and extorting or accepting cash payments from drug dealers in exchange for protecting them from arrest by law enforcement.

Earrey and his co-conspirator stole more than 1,000 pounds of marijuana from evidence and covered up the theft by submitting falsified paperwork showing that the drugs had been destroyed. Earrey, who had an addiction to prescription opiates, also used his corrupt activities to obtain illegal drugs for his own use. On one occasion, he traded cases of ammunition that he had diverted from the Florida Highway Patrol to a convicted murderer in exchange for oxycodone. Despite knowing that his drug addiction made it illegal for him to have firearms and ammunition, Earrey continued to possess these items in violation of federal law.
(Source)

DEA Agent Sentenced To Prison In Corruption Case / 3 Other Agents Convicted - August 12, 2021

Chad Scott was narcotics agent known as the "white devil" among drug traffickers. He was sentenced to more than 13 years in prison for stealing money from suspects, falsifying government records and committing perjury during a federal trial. The sentencing capped a 5 year case that shook the DEA and resulted in convictions of 3 other members of a New Orleans-based federal drug task force.

Prosecutors portrayed Scott as more dangerous than the most hardened heroin dealers he locked up, saying Scott broke every rule in the book to enforce his own approximation of justice.

Scott was found guilty at successive trials of a long list of corruption counts. The charges stemmed from an expansive federal investigation into misconduct claims that had surrounded Scott for much of his 17-year career, even as he racked up headline-grabbing drug busts between Baton Rouge and New Orleans.

At least a 12 DEA agents across the country have been criminally charged since 2015 on counts ranging from wire fraud and bribery to selling firearms to drug traffickers, according to court records. That includes a longtime special agent in Chicago who pleaded guilty to infiltrating the DEA on behalf of drug traffickers and another accused of accepting $250,000 in bribes to protect the Mafia. (Source)

DEA Public Affairs Officer Sentenced To Prison For $4 Million Fraud Scheme - Scamming Victims By Posing As A Covert CIA Officer - October 28, 2020

Garrison Courtney (Drug Enforcement Administration Public Affairs Officer) falsely claimed to be a covert officer of the CIA involved in a highly-classified program or task force involving various components of the U.S. Intelligence Community and the Department of Defense. The false story told by Courtney, was that a supposed classified program sought to enhance the intelligence gathering capabilities of the U.S. government. In truth, Courtney had never been employed by the CIA, and the task force that he described did not exist

By claiming to be a covert CIA officer involved in a bogus classified 'task force,' Courtney defrauded his victims out of over $4.4 million. (Source)

DEA Special Agent Sentenced To Prison For $9 Million+ 7 Year Scheme That Diverted Drug Proceeds From Undercover Money Laundering Investigations / Used Funds To Purchase Home, Cars, Jewelry - December 9, 2021

Jose Irizarry pleaded guilty on Sept. 14, 2020, to all counts in a 19-count indictment that included conspiracy to commit money laundering, honest services wire fraud, bank fraud, and aggravated identity theft.

The scheme began shortly after Irizarry filed for personal bankruptcy protection in 2010. Irizarry used his position as a special agent to divert approximately $9 million from undercover DEA money laundering investigations to himself and to co-conspirators. In return, Irizarry received bribes and kickbacks worth at least $1 million for himself and his family, which was used to purchase jewelry, luxury cars, and a home.

To carry out the scheme, Irizarry and his co-conspirators used a stolen identity to open a bank account under false pretenses and then utilized the account to receive diverted drug proceeds. The scheme lasted throughout Irizarry's assignments to the DEA's Miami Field Division and to its office in Cartagena, Colombia. (Source)

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)

ICE Officer Found Guilty Of Illegally Directing 250+ Government Vehicle Repairs Contracts To His Wife's Company - August 9, 2024

Jacquesc Polzin was formerly was employed as a deportation officer at U.S. Immigration and Customs Enforcement (ICE). During his employment at ICE, Polzin served as a vehicle control officer, whose job was to facilitate service and repairs for ICE vehicles.

From at least November 2017 to September 2020, Polzin illegally sent service and parts orders from ICE to a Santa Fe Springs-based automotive repair company named JNJ Auto Repair LLC. This company was registered to Polzin's wife.

At all relevant times, Polzin had a financial interest in this company. He was involved in establishing and investing in the business, shared estimates from competitors with JNJ Auto so that it could beat the price and win the ICE contract, and was paid by JNJ Auto.

In total, Polzin was involved in more than 250 transactions between ICE and JNJ Auto for ICE vehicles. Polzin performed these actions while hiding his connection to JNJ Auto. (Source)

ICE Deportation Officer Charged For Money Laundering $700,000 - April 11, 2024

Christopher Toral is an employee of the Department of Homeland Security (DHS), working as a Deportation Ifficer for Immigration and Customs Enforcement.

On three occasions in 2023, Toral allegedly transported a total of approximately $700,000 in exchange for cash payments. In each instance, he believed the monies were proceeds from drug transactions..

Toral transported $200,000 between Feb. 9 and 28, 2023, from Dallas to Houston, according to the charges. In early March 2023, he allegedly travelled from Newark, New Jersey, to Houston with $300,000 in U.S. currency. (Source)

U.S. MARSHAL SERVICE

Special Deputy U.S. Marshal Sentenced To Prison For $1.4 Million+ Romance Scam / Money Laundering Conspiracy - April 11, 2024

Isidore Iwuagwu is a Special Deputy United States Marshal and Department of Justice contractor providing security for critical Department of Justice facilities.

Between October 2015 and July 2021, Iwuagwu participated in a romance scam in which individuals contacted victims on social media platforms and dating sites, engaged in online relationships with the victims, then convinced victims to send large sums of money claiming the funds were needed for purported personal hardships or shipping costs for various imports.

Iwuagwu transmitted monetary instruments and funds to a place outside of the United States with the intent to carry out a specified unlawful activity.

Specifically, Iwuagwu 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. Iwuagwu laundered more than $1.4 million as a result of the conspiracy (Source)

U.S. SECRET SERVICE

U.S. Secret Service Problems Known Since 2014 - Senior Leadership Tended To Cover Up Problems, Rather Than Address Them - January 1, 2025

The assassination attempts against President-elect Donald Trump last year reportedly occurred after lawmakers and presidential administrations failed to address weaknesses within the Secret Service during the past decade.

Separate 2014 investigations by the White House and Congress found that the Secret Service was in crisis and pushed beyond its capabilities. Leadership also tended to cover up problems rather than address them, The Washington Post reported on December 31, 2024.

However, the Post reported that instead of being fixed, some Secret Service problems have grown worse. For example, the agency still lacks a sufficient number of agents. That has led to burnout and low morale, with many veteran agents leaving, the outlet said.

The results of the 2014 investigations were recommendations that included an increase in agent training and the hiring of fresh leadership. A White House-commissioned probe in 2014 urged that Secret Service agents who protect the president spend 25% of their work time in training. Since that time, though, those agents have spent between 3% and 7% percent in training, government records show.

A 180 page report by the bipartisan congressional task force released Dec. 10, 2024. is one of the most detailed looks so far into the July assassination attempt against Trump during a campaign rally in Pennsylvania and a second one in Florida two months later. (Source)

TRANSPORTATION SECURITY ADMINISTRATION (TSA)

TSA Employee Charged For Making Bomb Hoax At Airport - July 9, 2024

Tulsa International Airport Police received a report of a bomb threat on a handwritten note that was located in the pre-security side of the airport. Airport police immediately responded and secured the area and determined that there was no threat to public safety. Airport police then conducted an investigation where they identified a possible suspect and contacted the Tulsa FBI office. Tulsa FBI took over the investigation from that point forward and proceeded with their own investigation.

A TSA employee Sharon Devine left a note in the restroom on March 5, 2024, and March 23, 2024. The notes stated there was a bomb located in the airport. (Source)

TSA Officer Sentenced To Prison For Accepting $8000 In Bribes / Attempting To Smuggle Methamphetamine Through LAX Airport - December 9, 2022

Michael Williams is a former Transportation Security Administration (TSA) Officer was sentenced to 70 months in federal prison for smuggling what he believed was methamphetamine through Los Angeles International Airport (LAX) in exchange for a total of $8,000 in cash.

In 2020, authorities conducted undercover operations involving Williams, whom they suspected of helping smuggle narcotics past security checkpoints at LAX. During the operations, Williams met several times with a drug source to receive what he thought was methamphetamine.

Williams agreed to deliver the "methamphetamine" in a backpack to the drug source's accomplice in the men's restroom past the airport terminal's security checkpoint.

After taking possession of what he believed was real narcotics, Williams transported an unscreened package containing the fake methamphetamine beyond the TSA screening area and delivered the package to another individual. This individual, whom Williams did not know was a federal agent, on both occasions exchanged $4,000 in cash in the stalls of the men's restroom in the airport's secure area. (Source)

TSA Official Sentenced To Prison For Stealing $150,000 From Federal Worker's Compensation Program - September 9, 2021

Emmanuel Papas was injured on the job in 2004, when he served with the TSA at the Newark International Liberty Airport. apas began receiving federal worker's compensation benefits.

A subsequent federal investigation by TSA agents revealed that Emmanuel Papas was improperly receiving benefits because he was actively working at granite shops in the Myrtle Beach area from March 2009 through February 2020. Surveillance showed Papas working, interviews with various granite business employees confirmed that he worked at three Myrtle Beach-area retail granite shops, and deposits into Papas's bank account showed income from Myrtle Beach-area granite businesses. The investigation also revealed that Papas disguised his income by having his earnings either paid in cash or with checks made payable in his family members' names. Papas, who ultimately confessed, also completed at least eight federal forms attesting that he had no outside income and was, thus, eligible to continue to receive his benefits. The total loss to the federal government was just under $150,000. (Source)

DEPARTMENT OF DEFENSE (DoD)

DoD Contractor Agrees To Pay $628,000 To Settle False Claims Act Allegations - January 3, 2025

A Vermont company will pay $628,328 to resolve allegations that it sold substandard items to the United States Army.

The settlement resolves allegations that from July 13, 2018 through November 21, 2019, Live Wire, LLC made false claims in conjunction with contracts awarded to it by the United States Army. Live Wire contracted with the Army to sell electronic communications headsets and admits in the settlement that it provided non-compliant headsets that were not tested to the appropriate military specifications prior to their sale. Upon discovering that the headsets were not properly tested, Live Wire self-disclosed that information to the Government and cooperated with the investigation. (Source)

DoD Government Contractor Agrees to Pay $1M To Resolve False Claims Act Allegations For Submitting Fraudulent Bids On Prime Vendor Contracts - January 3, 2025

Johnny Buscema and his companies, S.A.F.E. Structure Designs, based in Las Vegas, and U.S.A. Manufacturing, based in New Port Richey, have agreed to pay $1,000,000 to resolve allegations that they violated the False Claims Act by causing a prime vendor for the Defense Logistics Agency (DLA) to submit fraudulent contract bids to DLA that resulted in Department of Defense (DoD) customers being overcharged for goods and related services purchased under those contracts. The settlement is based on the settling parties' ability to pay.

The United States alleged that, from 2016 to 2023, the settling parties conspired with other entities to rig bids for awards on the MRO contracts for the Northeast and Southeast regions of the United States.

More specifically, Buscema allegedly submitted non-competitive bids, paid other vendors to submit non-competitive bids and submitted multiple bids from his own two companies on the same solicitations to assist the prime vendor to meet its obligation to obtain bids from two or three vendors and to make one of the bids appear more competitive. As a result of these alleged schemes, the United States contends it was overcharged for items purchased under the MRO contracts. (Source)

Defense Of Department Employee Pleads Guilty To $624,000 Fake Invoices Scheme - July 1, 2024
Zelene Charles, a previous civilian employee of the Department of Defense, at the Defense Language Institute in Monterey, California, perpetrated a scheme to defraud the U.S. government by creating fake purchase requests and invoices for government purchases from both fictitious and legitimate business entities.

The items listed in these invoices were never actually purchased or received by the government. Between December 2016 and April 2020, Charles placed approximately 185 fraudulent charges, causing a total loss to the government of $624,250. To conceal that she was the recipient of the stolen funds, Charles frequently renamed the business names associated with intermediary accounts and, in total, used at least 78 different account names. (Source)

DoD Chief Information Officer Charged With Facilitating Dog Fighting Ring - October 2, 2023
Frederick Moorefield and Mario Flythe have been charged with promoting and furthering animal fighting venture.

Frederick Moorefield, a Deputy Chief Information Officer for Command, Control, and Communications, for Office of the Secretary of Defense, and Flythe used an encrypted messaging application to communicate with individuals throughout the United States to discuss dogfighting. Moorefield used the name "Geehad Kennels" and Flythe used the name "Razor Sharp Kennels" to identify their respective dogfighting operations.

For example, as detailed in the affidavit, Moorefield, Flythe and their associates used the encrypted messaging application to discuss how to train dogs for illegal dogfighting, exchanged videos about dogfighting, and arranged and coordinated dogfights. Moorefield and Flythe also discussed betting on dogfighting, discussed dogs that died as a result of dogfighting, and circulated media reports about dogfighters who had been caught by law enforcement. As further alleged in the affidavit, Moorefield and others also discussed how to conceal their conduct from law enforcement.

On September 6, 2023, law enforcement officers executed search warrants at Moorefield and Flythe's residences in Maryland. Following the execution of these warrants, twelve dogs were recovered and seized by the federal government. Law enforcement also recovered veterinary steroids, training schedules, a carpet that appeared to be stained with blood, and a weighted dog vest with a patch reading "Geehad Kennels." In addition, law enforcement officers seized a device consisting of an electrical plug and jumper cables, which the affidavit alleges is consistent with devices used to execute dogs that lose dogfights. (Source)

Defense Contract Management Agency Employee Pleads Guilty To Stealing Identities Of 37 Individuals To Commit $240,000+ Bank & Loan Fraud Scheme / Used Funds To Pay Debts / Bills- January 26, 2022
Kevin Lee used his position at the Defense Contract Management Agency (DCMA) to steal the identities of at least 37 individuals and using those identities to commit over $240,000 in bank and loan fraud.

From September 2018 to September 2020, Lee devised a scheme to defraud various banks and loan companies by using stolen identities to apply for and obtain loans, which he then used to pay personal debts and bills.

Lee initially used the identities of family members to apply for and obtain fraudulent loans. In September 2019, Lee began applying for loans and bank accounts using information he had access to as a result of his employment at DCMA. (Source)

DoD OIG Official Sentenced To Prison For Accepting Bribes For Telecommunications Contract- January 14, 2022

Matthew LumHo was employed at the DoD OIG's Information Services Directorate. In that position, LumHo oversaw and administered a prime federal contract designed to allow federal agencies in the National Capital Region to order routine telecommunications services and equipment from one of two national telecommunications companies.

Beginning no later than 2012, LumHo solicited and accepted bribes from co-conspirator William S. Wilson, in exchange for steering what nominally was intended to be telecommunications or information technology services through the prime government contract, through an intermediary telecommunications company, to Wilson's company. Wilson's company received all of this business without any competition, despite its lack of any relevant experience or expertise, and despite having no employees based in or near northern Virginia, where all the work was to be performed. Wilson and LumHo disguised the bribes by falsely masking them as payroll payments to a relative of LumHo for a job that did not in fact exist, with the bribes being deposited into an account that LumHo in fact controlled.

As the scheme progressed, LumHo, who was supposed to be safeguarding the contract, knowingly authorized numerous false and fraudulent service orders through the prime contract. The false service orders typically described the items supposedly being provided to the government as specialized IT-related support services, when in fact the co-conspirators were simply buying standard, commercially available items, dramatically marking up the price, and billing the government as though it had been provided with the specialized IT-related services. LumHo and Wilson also used fraudulent service orders to conceal bribes in the form of high-end camera equipment and stereo equipment sent from Wilson to LumHo, thereby defrauding the government into to paying for the very bribes themselves. (Source)

DoD Police Officer Sentenced To Prison For Over Billing DOD $25,000+ For Hours Not Worked - November 18, 2021

From at least August 2016 through October 2019, Anthony Lesane, a police officer working for the Department of Defense at a facility in Prince George's County, Maryland, falsely recorded work hours in his department's time and attendance system that he had not worked.

On most occasions, Lesane claimed to have worked overtime hours and on at least one occasion, Lesane claimed work hours while he was out of the country on vacation. Lesane stole at least $25,832.47 by overbilling the DoD. (Source)

Walter Reed (WR) Medcial Center Department Head Sentenced To Prison For Accepting Cash, Event Tickets & Other Gratuities From Company That Received More Than $25 Million in Government Business From WR - September 30, 2021

From 2009 until May 2019, David Laufer worked as the Chief of the Prosthetics and Orthotics Department at Walter Reed National Military Medical Center.

Bruce Thomas owned, operated, and controlled Pinnacle Orthopedic Services (Pinnacle). Pinnacle provided prosthetics and orthotics materials to Walter Reed in return for payments from the government.

Between 2012 and 2016, Laufer and his wife received things of value, that is the airlines travel, lodging and entertainment tickets, as well as direct cash payments, for and because of Laufer's official acts as the Chief of the Prosthetics and Orthotics department and Laufer's official acts in connection with the purchase of prosthetics and orthotics materials from Pinnacle. Laufer admitted that he undertook official acts in connection with the gratuities, including seeking renewal of Blanket Purchase Agreements (BPA's) with Pinnacle, sending multiple purchase requests obligating millions of dollars to Pinnacle for prosthetics and orthotics materials, and causing the BPA's repeated ordering of supplies from Pinnacle. (Source)

DoD Contractor Sentenced To Prison For Theft / Sale Of $150,000+ Of Military Equipment On U.S. Military Base in Afghanistan - April 27, 2021

Varita Quincy admitted that between April 2015 and July 2015, she and others conspired to and did steal property of value to the United States including generators, a truck, and other items worth over $150,000. Larry Green, one of her co-conspirators, negotiated the sale of the stolen property with a third-country national middleman, who in turn facilitated the sale of the items to unknown persons in Kandahar.

Quincy further admitted that, to effectuate the theft of the generators, she used her position as a security badging and escort pass supervisor to create or cause to be made false official documents. The false official documents facilitated both the entry of unknown and unvetted Afghan nationals and their vehicles on to the military installation and effectuated the removal of the stolen property from the installation. The falsified documents were used to deceive security officers and gate guards and compromised the security of U.S. military and civilian personnel on the military installation. (Source)

U.S. ARMY

U.S. Army Veteran Sentenced Prison For $779,000+ Of Disability Benefits Fraud - January 13, 2025

For nearly 14 years, Kevin McMains received over $779,000 in government disability benefits by providing false information to the Department of Veterans Affairs (VA).

McMains submitted fraudulent documentation and made false statements to medical professionals and in his applications claiming that post-traumatic stress was affecting his life to the extent he was unable to work, do normal daily activities, or care for himself, knowing that was not true. In addition, he also falsely claimed he was awarded a Purple Heart as proof of his service-connected injuries. As a result of his fraud, McMains also qualified for and received Social Security disability benefits and Medicare coverage to which he would not have otherwise been entitled.

In addition to a 33-month prison sentence, McMains was ordered to pay restitution of $378,380.82 to the VA, $357,847.80 to the SSA, and $43,451.56 to the Centers for Medicare and Medicaid Services. (Source)

U.S. Army Soldier Posing As Cyber Criminal Charged For Selling Customer Call Records Stolen From AT&T & Verizon - December 30, 2024

Federal authorities have arrested and indicted a 20-year-old U.S. Army soldier on suspicion of being Kiberphant0m, a cybercriminal who has been selling and leaking sensitive customer call records stolen earlier this year from AT&T and Verizon. (Source)

3 Individuals Plead Guilty In Conspiracy Scheme Involving The Bribery Of A U.S. Army Government Contracting Officer - December 19, 2024

Francisco Guerra, Coogan Preston and Jason Ingram pleaded guilty to conspiracy to bribe a public official. Preston also pleaded guilty to receiving a gratuity as a public official.

According to the plea agreements, the scheme began in 2016 and continued until 2021. As part of the scheme, Guerra agreed to provide money and other items of value to Preston, a government contracting official working at Redstone Arsenal in Huntsville, Alabama. In exchange for these bribes, Preston identified subcontracting opportunities for companies owned and operated by Guerra and convinced the prime contractor to use one of Guerra's companies as a subcontractor. (Source)

U.S. Army National Guard Soldier Charged With Murder - December 16, 2024

Natravien Landry is an Army National Guard soldier assigned to the 1148th Transportation Company at Fort Eisenhower.

He is alleged to have visited the residence in post housing at Fort Eisenhower early Saturday morning, Dec. 14, of a woman with whom Landry shares a child.

Landry is accused of assaulting and shooting a man who was with the woman in her residence, and then leaving Fort Eisenhower. Landry was arrested about three hours later south of Atlanta on Interstate 85 during a traffic stop by the Meriwether County, Georgia, Sheriff's Office, and deputies recovered a 9 mm pistol during the stop. (Source)

3 U.S. Army Soldiers Arrested On Human Smuggling Conspiracy Charges - December 4, 2024

3 Fort Cavazos soldiers were arrested on criminal charges related to their alleged involvement in a conspiracy to smuggle undocumented noncitizens.

The U.S. Border Patrol Agent initiated a vehicle stop in Presidio on Nov. 27. The vehicle fled as the agent approached the passenger side and struck a second USBP vehicle, injuring an agent inside, according to the filed criminal complaint. Presidio County Deputies and Presidio Police Officers eventually stopped the vehicle and apprehended four individuals, three of whom were undocumented noncitizens—one Mexican national and two Guatemalan nationals. The fourth individual was Emilio Mendoza Lopez, who claimed to be the front seat passenger in the vehicle. The driver, alleged to be Angel Palma, fled on foot and was located the following day at a hotel in Odessa.

Mendoza Lopez and Palma allegedly traveled from Fort Cavazos to Presidio for the purpose of picking up and transporting undocumented noncitizens. A third individual, Enrique Jauregui, is alleged to be the recruiter and facilitator of the human smuggling conspiracy. Data extracted from Palma's phone through a search warrant revealed messages between the three soldiers indicating collaboration in the smuggling operation.
(Source)

3 Active Duty U.S. Army Soldiers Convicted For Fraudulently Obtaining $100,000+ In COVID-19 Related Loans - December 3, 2024

Major Eduwell Jenkins, Sergeant First Class Crispin Abad and Sergeant Malaysia Stubbs filed for fraudulent PPP loans in 2021.

Though they were active-duty soldiers, Jenkins and Stubbs falsely represented to the Small Business Administration (SBA) that they each had jobs separate from their military employment that generated over $100,000 in annual income. To substantiate this false income, Jenkins and Stubbs generated fabricated Internal Revenue Service (IRS) tax return forms, submitting them to the SBA as supporting documentation for the PPP applications. Jenkins and Stubbs never submitted these falsified tax return forms to the IRS as part of legitimate tax filings. Based on their false submittals, Jenkins and Stubbs each received over $20,000 in government-backed PPP loans to which they were not entitled.

Abad allegedly received over $41,000 in PPP loans to which he was not entitled. Abad then allegedly used fraudulently obtained funds for various luxury and recreational spending, including purchases at the Fort Gregg-Adams Golf Course, Ace Adventure Resort in West Virginia, Victoria's Secret, Sunglass Hut, and the Virginia ABC Store. Additionally, Abad allegedly purchased jewelry at Reeds Jeweler and withdrew hundreds of dollars in fraud proceeds at the MGM Casino in National Harbor, Maryland. (Source)

U.S. Army Research Biologist Sentenced To Prison For Receiving $111,000+ In Bribes For Contracts / Used Funds For Rental Properties - November 5, 2024

Jason Edmonds was employed by the United States Army as a Research Biologist at the U.S. Army Combat Capabilities Development Command (CCDC) Chemical Biological Center (CB Center), located at the Aberdeen Proving Ground (APG).

The CCDC CB Center was the nation's principal research and development center for non-medical chemical and biological weapons defense. The CB Center developed technology in the areas of detection, protection, and decontamination.

From 2012 to 2019, Edmonds accepted cash and other financial benefits from John Conigliaro, the owner and CEO of EISCO, Inc. in exchange for favorable action on CB Center contracts. For example, in July 2013, Edmonds directed a $300,000 CB Center project to EISCO. Three months later, in October 2013, Conigliaro gave Edmonds $40,000 in cash so that Edmonds could purchase two rental real estate properties. Once Edmonds purchased the rental properties, Conigliaro paid for thousands of dollars of renovations to the rental properties.

Relative to the cash exchange, Edmonds and Conigliaro executed a "Promissory Note," which was subsequently amended by Edmonds on June 14, 2014. In the amended "Promissory Note," Edmonds credited himself $18,100 against the $40,000 in cash for past projects that Edmonds had directed to EISCO at the CB Center. Edmonds also wrote that Conigliaro would provide him an additional $25,000 in exchange for future projects that Edmonds would direct to EISCO.

Between December 2016 and August 2017, Edmonds directed a series of government projects to EISCO in exchange for a stream of benefits from Conigliaro, including a kitchen remodel at Edmonds's personal residence, the purchase of a granite countertop, a kitchen sink, and new siding to his home. (Source)

U.S. Army Reservist Pleads Guilty To Stealing $11,000+ Of Government Funds - September 30, 2024
United States Army Reservist Cody Francis pled guilty to conspiracy to commit theft of government funds.

Francis stole $11,378.27 from the United States Department of the Army, by claiming reimbursement for performing military funeral honors ceremonies that never actually happened. (Source)

U.S. Army Recruiter Charged With $266,000 Bank Fraud And Identity Theft Scheme Using Army Recruits PII - September 11, 2024
Jane Crosby was a Sergeant First Class in the U.S. Army and U.S. Army recruiter. She has been charged for engaging in a fraudulent scheme to defraud a credit union by using her position to obtain the personally identifying information of U.S. Army recruits and recruit candidates and submit fraudulent bank account applications to the credit union on the recruits'.

From Sept. 12, 2023, to Dec. 27, 2023, Crosby submitted "Pre-Active Duty Membership" bank account applications to a credit union on behalf of seven U.S. Army recruits or purported recruits, without their knowledge or consent. Such accounts are intended to facilitate the direct deposit of soon-to-be service members' salaries once they join the military. These applications included the victims' names and Social Security numbers as well as copies of their passports, driver's licenses, and/or Social Security cards. Once these credit union accounts were opened, Crosby, posing as the victims, applied for approximately $266,000 in loans and credit card accounts and used some of the accounts to deposit fraudulent checks and then withdraw funds. (Source)

U.S. Army Soldier Charged With Unlawful Firearms Trafficking And Lying About His Involvement in Insurrectionist Groups - August 19, 2024
On Aug. 14, 2024, Kai Liam Nix, also known as Kai Brazelton was charged with unlawful firearms trafficking, including the sale of two stolen firearms. Nix was also charged with making a false statement to the government. Nix is an active-duty U.S. Army soldier, stationed at Fort Liberty in Fayetteville, North Carolina. He was arrested on Aug. 15 and made his initial appearance in court today.

According to the court documents, Nix made a false statement on his Security Clearance Application Standard Form (SF) 86 when he claimed he had never been a member of a group dedicated to the use of violence or force to overthrow the U.S. Government. (Source)

U.S. Army Financial Counselor Sentenced To Prison For Defrauding Families Through Investment Scheme Which Earned Him $1.4 Million In Commissions - August 21, 2024
From November 2017 to January 2023, Caz Craffy was a civilian employee of the U.S. Army, working as a financial counselor with the Casualty Assistance Office. He was also a Major in the U.S. Army Reserves, where he has been enlisted since 2003. Craffy was responsible for providing general financial education to the surviving beneficiaries. He was prohibited from offering any personal opinions regarding the surviving beneficiary's benefits decisions. Craffy was not permitted to participate personally in any government matter in which he had an outside financial interest. However, without telling the Army, Craffy simultaneously maintained outside employment with two separate financial investment firms.

Craffy used his position as an Army financial counselor to identify and target Gold Star families and other military families. He encouraged the Gold Star families to invest their survivor benefits in investment accounts that he managed in his outside, private employment.

Based upon Craffy's false representations and omissions, the vast majority of the Gold Star families mistakenly believed that Craffy's management of their money was done on behalf of and with the Army's authorization.

From May 2018 to November 2022, Craffy obtained more than $9.9 million from Gold Star families to invest in accounts managed by Craffy in his private capacity. Once in control of this money, Craffy repeatedly executed trades, often without the family's authorization. These unauthorized trades earned Craffy high commissions. During the timeframe of the alleged scheme, the Gold Star family accounts had lost more than $3.7 million, while Craffy personally earned more than $1.4 million in commissions, drawn from the family accounts. (Source)

U.S. Army Intelligence Analyst Pleads Guilty To Charges Obtaining & Disclosing Classified Information To Individual Associated With Chinese Government - August 13, 2024

Korbein Schultz, a U.S. Army soldier and Intelligence Analyst, pleaded guilty with conspiracy to obtain and disclose national defense information, exporting technical data related to defense articles without a license, conspiracy to export defense articles without a license, and bribery of a public official.

Schultz held a Top Secret / Sensitive Compartmented Information (TS/SCI) security clearance. He conspired with an individual who lived in Hong Kong and who Schultz suspected of being associated with the Chinese Government (Conspirator A) to collect national defense information, including classified information and export-controlled technical data related to U.S. military weapons systems, and to transmit that information to Conspirator A in exchange for money. Schultz entered into this conspiracy even though, as part of his official duties in the Army, he was required (1) to protect national defense information, classified information, and controlled unclassified information (CUI); (2) to train other members of his unit on the proper handling, storage, and dissemination of classified information and information marked CUI; and (3) to report suspicious incidents,

including attempts by anyone without authorization to receive classified or sensitive information about U.S. military operations, organizations, equipment, or personnel. (Source)

U.S. Army Contracting Officer Sentenced To Prison For $490,000 4 Year Contracting Fraud Scheme To Live Luxury Lifestyle - August 6, 2024

Thomas Bouchard was the Contracting Officer in charge of the U.S. Army Natick Contracting Division, in Massachusetts.

In 2014, Bouchard used his long-standing relationship with Evolution Enterprise, Inc., a government contractor, to have Chantelle Boyd hired for a "no show" job as an assistant that specifically supported Bouchard. Boyd's position cost the Department of Defense more than $490,000 during her time at Evolution from 2014 to 2018, during which Boyd performed little if any useful function.

Bouchard and Boyd took numerous government-funded trips, ranging in duration from two to 15 days, under the guise that they were work related. This included 31 trips to Orlando, Fla., among other locations such as Clearwater Beach, Fla., and Stafford, Va., during which Boyd performed little if any work. For many of the trips, Bouchard and Boyd stayed in the same hotel room and spent time at the pool and Disney parks – all during business hours. In order to conceal the personal nature of the trips, Bouchard altered, created and approved false travel to reimburse the Boyd for out-of-pocket expenses. (Source)

U.S. Army Officer Sentenced To Prison For Role In Theft Of Government Property Theft That Profited Him $2 Million+ - July 24, 2024

Chief Warrant Officer Three (CW3) Christopher Hammond used his position to requisition government property intended for his unit at then Ft. Bragg, now called Ft. Liberty.

The property was never logged into inventory at the base but was instead sold by Hammond to various individuals. In a two-year period, CW3 Hammond received at least $1.8 million in wire transfers and other payments related to the sales, which he deposited into bank accounts controlled by him and his wife. A search warrant executed at Hammond's home resulted in the seizure of at least 98 firearms, at least 90 military-issued spotting scopes, hundreds of other military-issued firearm accessories and items including night vision goggles and electronic equipment, and more than $100,000 in cash.

The investigation traced about 200 items sold by CW3 Hammond or held in his home as having been issued to Hammond's military unit. The fraud was uncovered when a supplier noticed that items procured under a government contract were being sent in for warranty repairs by a private individual. Hammond's wife, Major Heather Hammond, was also charged by the government, but was ultimately acquitted by a jury. (Source)

U.S. Army Officer / JAG Attorney Pleads Guilty To Destruction Of U.S. Army Property & Lying To Investigators About Contacting Russian Embassy - July 24, 2024

In February 2022, Manfredo Madrigal was assigned to a staff position at the Judge Advocate General (JAG) School in the Training Developments Directorate, whose mission was to design and develop training products for the JAG Corps and the Army. Madrigal possessed an active security clearance and previously served overseas on sensitive operations.

In early 2022, Madrigal was under investigation by the U.S. Army and the JAG School for failing to report a previous conviction for driving under the influence (DUI).

While his Army investigation was pending, Madrigal deleted, without authorization, online JAG training materials and filmed himself doing so while graphically describing his ill-will towards the Army. The FBI's investigation also revealed that Madrigal made a phone call to the Russian embassy in Washington, DC the same night that he deleted the training materials and then texted a witness that Russia wanted to know what he knew.

On February 22, 2022, Madrigal was discharged from the JAG School and claimed in his exit paperwork that he had no unreported contact with a foreign national. In April and May 2022, Madrigal was interviewed by the FBI about his actions. In these interviews, Madrigal made multiple false statements regarding his actions, including denying any involvement in the deletion of materials and that he only learned of the deletion from a coworker, as well as falsely denying his contact with a foreign national at the Embassy. (Source)

U.S. Army Civilian Employee Sentenced To Prison For $100 Million Fraud Scheme / Used Funds For Jewelry, Clothing, Vehicles, Real Estate - - July 23,2024

Janet Mello worked as a Financial Program Manager for the U.S. Army, Installation Management Command – G9 (Morale, Welfare and Recreation) Child and Youth Services (CYS) at Fort Sam Houston, in Texas

In or around December 2016 through at least August 29, 2023, Mello formed a business she called Child Health and Youth Lifelong Development (CHYLD). The sole purpose of CHYLD was to receive grant funds from the 4-H Military Partnership Grant program, which Mello fraudulently secured by way of her position as a CYS financial program manager.

Once Mello received a grant check, she deposited the check into her bank account, spending the money on clothing, jewelry, vehicles and real estate. Mello repeated the process 49 times during a six-year period, requesting approximately $117,000,000 in payments, and receiving approximately $108,917,749. (Source)

U.S. Army Reserve Officer Admits To Military Pay Fraud Of $140,000+ - July 19, 2024

Captain Jean Philippe Martial worked as a U.S. Army Reservist from Utah's 76th Operational Response Command. He was indicted for military pay fraud that occurred at Fort Douglas, Utah, during the coronavirus pandemic.

Captain Martial defrauded the United States out of more than $140,000 in unearned military pay entitlements from June 2019 to September 2021. Last month, Colonel Reece Roberts, formerly of Utah's 76th Operational Response Command, pled guilty to filing a fraudulent claim against the United States, conspiring to defraud the United States, and other federal crimes. (Source)

8 U.S. Army Civilian Employees Sentenced To Prison For Stealing Government Property Worth Millions From Army Depot & Delivering To Military Surplus Store To Sell - May 30, 2024

8 Army Civilian Employees have been sentenced to prison for conspiring to steal United States property from Anniston Army Depot (ANAD), in Alabama.

These civilian employees at ANAD stole millions of dollars in military property from warehouses at the depot over a period of several years and delivered it to middlemen. The middlemen delivered the stolen property to the owner of a military surplus store to sell. The conspirators split the money from the sale of the stolen property. The stolen items included equipment that was designed to be attached to military weapon systems to provide operators with instant nighttime engagement capabilities and/or improved target acquisition. (Source)

U.S. Army Lieutenant Colonel Charged With Arms Export Control Act Violations - May 3, 2024

Frank Talbert is a Lieutenant Colonel with U.S. Army Explosives Ordinance Disposal (EOD) assigned to Fort Campbell.

He is facing federal criminal charges after law enforcement officers conducted an investigation and executed multiple search warrants uncovering evidence that Talbert unlawfully imported firearms parts from Russia and other countries, unlawfully dealt in firearms without a federal firearms license, and committed multiple firearms violations related to the possession of machineguns. (Source)

U.S. Army Major Found Guilty After Smuggling Guns To Ghana - April 29, 2024

A federal jury convicted a United States Army Major (Kojo Dartey), currently assigned to Fort Liberty, on charges of dealing in firearms without a license, delivering firearms without notice to the carrier, smuggling goods from the United States, illegally exporting firearms without a license, making false statements to an agency of the United States, making false declarations before the court, and conspiracy.

Between June 28 and July 2, 2021, Dartey purchased seven firearms in the Fort Liberty area and tasked a U.S. Army Staff Sergeant at Fort Campbell, Kentucky, to purchase three firearms there and send them to Dartey in North Carolina. Dartey then hid all the firearms, including multiple handguns, an AR15, 50-round magazines, suppressors, and a combat shotgun inside blue barrels underneath rice and household goods and smuggled the barrels out of the Port of Baltimore, Maryland, on a container ship to the Port of Tema in Ghana.

The Ghana Revenue Authority recovered the firearms and reported the seizure to the DEA attaché in Ghana and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Baltimore Field Division. At the same time, Dartey was a witness in the trial of U.S. v. Agyapong. A case that involved a 16-defendant marriage fraud scheme between soldiers on Fort Liberty and foreign nationals from Ghana that Dartey had tipped off officials to. In preparation for the trial, Dartey lied to federal law enforcement about his sexual relationship with a defense witness and lied on the stand and under oath about the relationship. (Source)

U.S. Army Reservist Sentenced To Prison For Theft Of $11,000+ From Government - April 26, 2024

Leroy Daniels stole $11,693.87 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never occurred. (Source)

U.S. Army Service Member Sentenced To Prison In Money Laundering Romance Scam - April 18, 2023

Sanda Frimpong, wa an active duty servicemember stationed at Fort Bragg.

Frimpong was arrested after the unsealing of a 19-count indictment that included charges of Money Laundering,Fraud, Conspiracy, Aggravated Identity Theft, and Access Device Fraud in connection with multiple interstate and international fraud and money-laundering scams.

Frimpong and other conspirators, engaged in elaborate scams, impersonating romantic love interests, diplomats, customs personnel, military personnel, and other fictitious personas for the purpose of ensnaring their victims by earning their confidence, including promises of romance, sharing of an inheritance or other riches, or other scenarios intended to fraudulently induce the victims to provide money or property to the conspirators. Frimpong allegedly laundered hundreds of thousands of dollars in proceeds of these frauds through his various bank accounts across state lines and through contacts in Ghana. (Source)

U.S. Army Reserve Officer Pleads Guilty To $488,000+ COVID Relief Fraud Scheme / Used Funds For Investment Ventures & To Pay Debts - March 6, 2024

Russell Laraway, an Army Reserve officer, incorporated two business entities in Virginia that he purported to operate out of his home in Leesburg: Loudoun Innovation LLC ("LI LLC") and Commonwealth Commerce LLC ("CC LLC"). Beginning in April 2020, Laraway submitted loan applications through the Paycheck Protection Program (PPP), a COVID-19 relief program that was intended to provide loans backed by the Small Business Administration to certain businesses, nonprofit organizations, and other entities to help them retain their employees or stay afloat during the pandemic. In his applications, Laraway inflated the numbers of people his business entities employed and falsified payroll expenses and revenues for each company.

Laraway sought loan forgiveness for some of the PPP loans by falsely certifying that the PPP money had been used solely for payroll or other authorized purposes, while he actually intended to use the money to engage in spurious investment ventures and pay off personal debts. Laraway fraudulently received two PPP loans for LI LLC and two PPP loans for CC LLC. The four PPP loans totaled approximately $488,952, some of which Laraway paid to foreign entities in scams of which he was a victim. (Source)

U.S. Army Soldier Sentenced To Prison For Role In Drug Trafficking And $700,000+ In Money Laundering - January 26, 2024

On May 7, 2021, U.S. Homeland Security Investigations was notified by the French Customs Service stationed at Charles De Gaulle International airport that a package from Cameroon had been intercepted containing approximately three kilograms of ketamine.

The package was delivered to Gordon Ray Custis, then a soldier at Fort Liberty, at his home in Fayetteville, by Federal Task Force Officers with the Cumberland County Sheriff's Office.

Custis pled guilty to possession with the intent to distribute ketamine and he was released pending sentencing. While awaiting sentencing, the Army Criminal Investigative Division and Defense Criminal Investigative Service received information that Custis was laundering money. The subsequent investigation revealed that Custis, acting in a leadership role involving co-defendant and others, laundered over $700,000.

On February 1, 2023, a second search warrant was executed at Custis's home and investigators recovered 28.5 kilograms of ketamine, $164,200 in cash, digital scales and vacuums sealing materials. (Source)

U.S. Army Maintenance Worker Pleads Guilty To Using Fuel Credit Card To Make $33,000+ Of Un-Authorized Fuel Purchases - November 14, 2023

Normas Dais was employed by the United States Army as a civilian maintenance worker at the Fort Lesley J. McNair Department of Public Works.

Dais repeatedly purchased gasoline for private vehicles using a General Services Administration fuel credit card meant solely for a designated maintenance van on the Fort McNair grounds. Investigators found that from April to October of 2023, Dais frequently arranged to meet private vehicles at area gas stations and used his General Services Administration credit card to purchase their gas. In total, Dais made more than 400 unauthorized purchases totaling at least $33,868.21. As part of the plea agreement, Dais agreed to pay full restitution. (Source)

U.S. Army Reservist Pleads Guilty For Role In Stealing $101,000+ Of Government Funds - October 13, 2023

Starting in January 2013, and continuing until in or about August 2016, Christopher O'Connor and co-conspirators conspired to obtain money from the Army under false pretenses by submitting false applications to the Army for military funeral honors (MFH) payment requests for services that had not been performed.

O'Connor proposed submitting false MFH pay requests in the co-conspirators' names in exchange for each sharing their proceeds with O'Connor. In addition to receiving a split of the fraudulent MFH payments from the co-conspirators, O'Connor also submitted and received approximately $18,825.83 in fraudulent MFH payment requests for himself. As a result of this conspiracy, the United States government was defrauded out of approximately $101,858.19.

The National Defense Authorization Act of 2000 authorizes MFH for active-duty soldiers, retirees, and veterans. At a family's request, eligible persons can receive military funeral honors, including the folding and presenting of the United States flag and the playing of Taps. (Source)

U.S. Army Sergeant Charged For Efforts To Give Classified Information To China - October 6. 2023

A former U.S. Army sergeant was arrested Friday at the San Francisco airport and indicted on charges that he unlawfully retained classified information and attempted to deliver it to China's security services, the Justice Department announced.

29, served as an active duty soldier between 2015 and 2020 with his primary assignment at Joint Base Lewis-McChord in Washington state, prosecutors said. In his role, Schmidt had access to SECRET and TOP SECRET information.

After his separation from the military, Schmidt allegedly reached out to the Chinese Consulate in Turkey and later, the Chinese security services via email offering information about national defense information.

In March 2020, Schmidt traveled to Hong Kong and allegedly continued his efforts to provide Chinese intelligence with classified information he obtained from his military service. He allegedly retained a device that allows for access to secure military computer networks and offered the device to Chinese authorities to assist them in efforts to gain access to such networks. (Source)

U.S. Army Reservist Pleads Guilty To Stealing $15,000 Of Government Funds - August 23, 2023
U.S. Army Reservist Derrick Branch pled guilty to conspiracy to commit theft of government funds.

Branch stole $15,469.30 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Reservist Sentenced To Prison For Stealing $21,000+ Of Government Funds - June 16, 2023
Lynea Sanders is a former United States Army Reservist.

Sanders pled guilty to conspiracy to commit theft of government funds, having stolen $21,780.18 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Reservist Sentenced To Prison For Stealing $8,300+ Of Government Funds - June 16, 2023
Chantelle Davis is a forrmer United States Army Reservist.

Davis pled guilty to conspiracy to commit theft of government funds, having stolen $8,399.65 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Soldier Pleads Guilty To Terrorism Charges For Attempting To Assist ISIS To Conduct Deadly Ambush On U.S. Troops - June 14, 2023
Cole Bridges joined the U.S. Army in approximately September 2019 and was assigned as a cavalry scout in the Third Infantry Division based in Fort Stewart, Georgia.

Beginning in at least 2019, Bridges began researching and consuming online propaganda promoting jihadists and their violent ideology. Bridges also expressed his support for ISIS and jihad on social media. In or about October 2020, Bridges began communicating with a Federal Bureau of Investigation (FBI) online covert employee (The OCE), who was posing as an ISIS supporter in contact with ISIS fighters in the Middle East. During these communications, Bridges expressed his frustration with the U.S. military and his desire to aid ISIS. Bridges then provided training and guidance to purported ISIS fighters who were planning attacks, including advice about potential targets in New York City. Bridges also provided the OCE with portions of a U.S. Army training manual and guidance about military combat tactics, for use by ISIS.

In or about December 2020, Bridges began to supply the OCE with instructions for the purported ISIS fighters on how to attack U.S. forces in the Middle East. Bridges diagrammed specific military maneuvers intended to help ISIS fighters maximize the lethality of attacks on U.S. troops.

Bridges further provided advice about the best way to fortify an ISIS encampment to repel an attack by U.S. Special Forces, including by wiring certain buildings with explosives to kill the U.S. troops. Then, in January 2021, Bridges provided the OCE with a video of himself in his U.S. Army body armor standing in front of a flag often used by ISIS fighters and making a gesture symbolic of support for ISIS. Approximately a week later, Bridges sent a second video in which Bridges using a voice manipulator, narrated a propaganda speech in support of the anticipated ambush by ISIS on U.S. troops.(Source)

3 Individuals (2 Of Them U.S. Army Police Officers) Are Charged In Role With Conspiracy To Steal Government Property From Army Depots - May 25, 2023

Kelvin Battle, Steve Bonner and Shane Farthing are each charged with one count of conspiracy to steal United States property. Battle and Bonner are also each charged with an additional count related to specific instances of stealing or selling property stolen from the Anniston Army Depot (ANAD). Six other individuals have pleaded guilty or agreed to plead guilty to offenses related to the theft of property from ANAD.

Battle and Farthing, who were police officers at ANAD, and other civilian employees of the Directorate of Emergency Services stole military property from warehouses at ANAD. Bonner acted as a middleman, selling stolen property directly to buyers and delivering stolen property to the owner of a military surplus store in Sylacauga. The stolen items included equipment that was designed to be attached to military weapon systems to provide operators with instant nighttime engagement capabilities and/or improved target acquisition. (Source)

U.S. Army Employee Arrested For Accepting $400,000+ In Bribery And Kickback Scheme Involving Defense Contracts - May 15, 2023

Young Kim while acting in his capacity as Chief of the Design Branch (2017-2021) at Army Garrison Yongsan / Casey in Korea (USAG-Y/C), developed a scheme to enrich himself through bribes and kickbacks from various manufacturers and suppliers of parts used in U.S. Army contracts.

While acting in that capacity, Kim helped ensure that certain Army contracts included the use of parts manufactured or supplied by specific companies. Some of these parts included blast doors, blast valves, shock mounts, and shock isolators (Equipment Designed To Protect Army Personnel In The Event Of An Attack). In return, the companies manufacturing or supplying those parts collectively sent over $400,000 in kickbacks to Kim. A significant portion of these funds were laundered through bank accounts controlled by Kim's adult relatives, including one account held in the name of a shell company and were ultimately used to enrich Kim and to pay for bills and expenses incurred by Kim. (Source)

U.S. Army Solider Sentenced To Prison For Role In $3.5 Million+ COVID-19 Fraud Scheme - January 9, 2023

Dara Buck, a U.S. Army Chief Warrant Officer, stationed at Fort Stewart, has been sentenced to federal prison for leading a prolific fraud scheme in which she and others illegally raked in millions of dollars from COVID-19 relief programs and federal student loan forgiveness.

From August 2017 through May 2021, Buck led a conspiracy to fraudulently obtain funding from the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Paycheck Protection Program (PPP), and to secure the fraudulent discharge of federal student loans using falsified disability claims.

Buck admitted submitting more than 150 fraudulent PPP loan applications to the Small Business Administrating for herself and others in the conspiracy, resulting in more than $3 million in fraudulent disbursements from banks to members of the conspiracy. Buck directly received fraudulently obtained PPP funding, or was paid by conspirators for submitting their fraudulent applications.

In addition, conspirators paid Buck to submit falsified U.S. Department of Veterans Affairs certifications for total and permanent disability to the U.S. Department of Education in order to fraudulently secure the discharge of more than a dozen student loans totaling more than $1 million. (Source)

U.S. Army Major And Wife Tried To Leak Military Health Data To Help Russia Gain Insights Into The Medical Conditions Of U.S. Military - September 29, 2022

Jamie Lee Henry, the former U.S. Army Major who was also a doctor at Fort Bragg in North Carolina, and his wife, Dr Anna Gabrielian, were charged in an unsealed indictment in a federal court in Maryland with conspiracy and the wrongful disclosure of individually identifiable health information about patients at the Army base.

The indictment alleges that the plot started after Russian President Vladimir Putin invaded Ukraine.

Prosecutors said the pair wanted to try to help the Russian government by providing them with data to help the Putin regime gain insights into the medical conditions of individuals associated with the US government and military.

The two met with someone whom they believed was a Russian official, but in fact was actually an FBI undercover agent.

At a hotel in Baltimore on Aug 17, Dr. Gabrielian told the undercover agent she was motivated by patriotism toward Russia to provide any assistance she could to Russia, even if it meant being fired or going to jail.

In the meeting, she volunteered to bring her husband into the scheme, saying he had information about prior military training the United States provided to Ukraine, among other things.

At another meeting later that day, Henry told the undercover agent he too was committed to Russia, and claimed he had even contemplated volunteering to join the Russian army. (Source)

4 U.S. Army Depot Officials & Vendors Sentenced To Prison For $7 Million+ Bribery And Conspiracy Scheme - September 13, 2022

Jimmy Scarbrough was the Equipment Mechanic Supervisor at the Red River Army Depot (RRAD) in Texarkana, Texas, a position he held from November 2001 until May 2019.

Scarbrough directed more than $7 million in purchases from RRAD to RRAD Vendor Jeffrey Harrison and Justin Bishop through the government purchase card (GPC) program. In order to manipulate the GPC program, which is designed to ensure a competitive bidding process, Scarbrough told the vendors what to bid, including the item, the quantity, and the price. By collecting fake bids from multiple vendors, Scarbrough was able to direct RRAD purchases to his select vendors, in this case Harrison and Bishop, while maintaining the appearance of a competitive bidding process. Scarbrough also defrauded the United States by falsely certifying that he had received the purchased items, therefore causing the RRAD to pay his select vendors. However, the reality was that Scarborough instructed the vendors not to deliver certain RRAD-purchased items.

Scarbrough demanded hundreds of thousands of dollars in bribes from his selected vendors. Scarbrough accepted bribes in various forms, including receiving at least $116,000.00 in U.S. Postal Service money orders from Harrison. Scarbrough also had Harrison and Bishop purchase at least $135,000.00 in car parts or services for his hot rod collection, which included a red and black 1936 Ford Tudor, an electric green 1932 Ford Coupe, a cherry red 1951 Ford F-1 truck, and more. Scarbrough received more than $27,000.00 worth of firearms from Bishop, including rare Colt handguns and Wurfflein dueling pistols. Finally, Scarbrough directed at least $32,000.00 in donations to the Hooks Volunteer Fire Department while he was the Capitan of Operations. In total, Scarbrough received more than $300,000.00 in bribe payments from Harrison and Bishop.

Scarbrough is not the only official at RRAD who accepted bribes. Devin McEwin accepted more than $21,000.00 in bribes from Harrison, including hunting trips, donations directed to the Annona Volunteer Fire Department, and the refurbishment of his 1964 Ford truck. Additionally, Louis Singleton accepted more than $18,000 in bribes from Harrison and others, including tickets to the Hall of Fame section of AT&T Stadium for the Dallas Cowboys football game against the New England Patriots. Singleton was the supervisor of the GPC program at the RRAD and was responsible for approving purchases requested by Scarbrough. (Source)

U.S. Army Employee Charged For Theft Of $800,000+ Of Military Heavy Equipment - May 10, 2023

From a time unknown but no earlier than November 1, 2021, and continuing through approximately December 31, 2021, Tamilo Fe'a stole military heavy equipment, including vehicles, semi-trailers, generator trailers, flatbed trailers, refrigerator trailers, armored office trailers, tractors, and box vans from the Hawthorne Army Weapons Depot in Hawthorne, Nevada.

The total value of the stolen property was over $800,000.00. From September 2020 to August 2021, Fe'a made about 69 transactions with a fuel fleet credit card for his personal benefit at various gas stations in Nevada, Arizona, New Mexico, and California. (Source)

U.S. Army Reservist Working Under The Direction Of A Chinese State Intelligence Unit Sentenced To Prison For Spying In An Effort To Steal Aviation Trade Secrets - January 26, 2023

A Chinese engineer has been jailed for eight years for spying in the U.S., in a case linked to Chinese efforts to steal aviation trade secrets.

Ji Chaoqun had identified scientists and engineers for possible recruitment, according to the DOJ. He also enlisted in the U.S. Army Reserves and lied to recruiters.

Authorities said Ji worked under the direction of a key Chinese State Intelligence Unit. Last September he was convicted for acting as an agent of a foreign government without notifying the U.S. and of making false statements to the Army. Ji had arrived in the U.S. on a student visa a decade ago, according to the DOJ. He was accused of supplying information to the Jiangsu Province Ministry of State Security about eight individuals for possible recruitment. (Source)

U.S. Army Procurement Agent Sentenced To Prison For Accepting $773,000 Of Bribes For Contracts - May 18, 2022

Calvin Jordan was a Procurement Agent assigned to the Operations and Maintenance Division, Directorate of Public Works (DPW), at Fort Bragg, NC. To obtain services, a Ft. Bragg facilities user submits a request for a repair or service of a facility, such as a roof leak, damaged floor, or plumbing issue to the DPW. The request creates a Demand Maintenance Order (DMO) that is forwarded to the appropriate commodity section.

The DMO is assigned to a DPW technician that specializes in a certain trade, such as roofing, flooring, plumbing, or carpentry.

From 2011 into 2019, Jordan used his position as a Procurement Agent to receive bribes of approximately $200 per DMO from various vendors contracting with DPW, Ft. Bragg, North Carolina, in return for increasing the number of federal contracts given the vendor. It is estimated Jordan received $773,600 in illegal bribes. (Source)

U.S. Army Purchasing Agent Sentenced To Prison For Role With Wife In $6 Million Embezzlement Scheme And Theft Of Government Property - June 9, 2021

Morris Cooper was a purchasing agent assigned to the Operations and Maintenance Division, Directorate of Public Works (DPW), at Fort Bragg, NC. He was entrusted to purchase HVAC parts for DPW's HVAC maintenance section.

Cooper was named in an indictment filed on August 20, 2019, which charged that he used his position as purchasing agent in the DPW on Ft. Bragg to receive cash and gifts for both him and his wife, Beverley Cooper, from vendors in return for steering contracts for supplies to those vendors. Additionally, he at times inflated the prices for items under those contracts beyond market price, increasing both the profits to the vendor and the cash payment made to Cooper and / or his wife.

Beverley Cooper was also charged with conspiring to steal government property and aiding and abetting Cooper to do so and was sentenced to 5 years probation.

They were ordered to pay $6,300,000 in restitution and an order of forfeiture was entered in the amount of $1,283,135.15, the amount they agreed they personally profited from the conspiracy. (Source)

U.S. Army Employee Sentenced To Prison For Kickback Scheme To Steer $3 Million+ Of U.S. Government Contracts - November 10, 2021

A former civilian employee of the U.S. Army's Directorate of Public Works was sentenced to two years in prison for a kickback scheme to steer government contracts for work at Camp Arifjan, a U.S. Army base in Kuwait.

Ephraim Garcia admitted that he conspired with Gandhiraj Sankaralingam, the former general manager and co-owner of Kuwait-based contracting company Gulf Link Venture Co. W.L.L. (Gulf Link), to steer government contracts to Gulf Link.

In his position with the U.S. Army, Garcia was involved in the solicitation, award and management of certain government contracts related to facilities support at Camp Arifjan.

In 2015, at an Olive Garden restaurant located in Mahboula, Kuwait, Garcia and Sankaralingam approached an employee of the prime contractor responsible for base support services. During that meeting, they offered to pay the prime-contractor employee in exchange for his assistance in steering subcontracts worth over $3 million to Gulf Link. Rather than agree to the scheme, the prime-contractor employee reported the kickback offer to authorities. (Source)

U.S. Army Contractor Sentenced To Prison For Stealing $1.5 Million From Military Members / Dependants In Scheme That Targeted 3,300+ U.S. Service Members & Veterans - October 1, 2021

Fredrick Brown was sentenced for one count of conspiracy to commit wire fraud and one count of conspiracy to commit money laundering following Brown's guilty plea on Oct. 29, 2019.

Brown conspired with four other individuals to steal money belonging to military members, and military dependents and civilians employed by the U.S. Department of Defense. The scheme targeted over 3,300 members of the U.S. military community resulting in $1.5 million in losses.

Brown, a former civilian medical records technician and administrator with the U.S. Army at the 65th Medical Brigade, Yongsan Garrison, South Korea, admitted that between July 2014 and September 2015, he stole the personal identifying information (PII) of thousands of military members, including names, Social Security numbers, military ID numbers, dates of birth and contact information.

Brown also admitted to capturing the PII by taking digital photographs of his computer screen while he was logged into a military electronic health records database and, subsequently, providing the stolen data to Philippines-based co-defendant Robert Wayne Boling Jr. Boling and others, who used the information to access DOD and Veterans Affairs benefits sites and steal millions of dollars. (Source)

U.S. Army National Guardsman & DoD Subcontractor Charged Conspiring To Steal And Sell Military Gear / Uniforms - August 19, 2021

Brandon Schulte are accused of conspiring with each other and others unnamed to steal military uniforms, tactical robots, night vision sights, high frequency radios, and other functional military equipment.

Jody Stambaugh and Joe Stambaugh were co-owners of Stambaugh Enterprises, a scrap metal company. Stambaugh Enterprises allegedly operated as a subcontractor on a DoD contract to pick-up, transport, and recycle scrap metal items from multiple DoD facilities in Illinois and Missouri, including Scott Air Force Base in St. Clair County, Illinois, and a Missouri Army National Guard facility in Jefferson City, Missouri.

The Stambaughs were obligated to mutilate and destroy all military property they hauled away from each DoD facility and were prohibited from reusing or refurbishing any military items for their own use or selling any military items to be reused or refurbished by someone else.

The Stambaughs allegedly removed truckloads of military property from DoD facilities but did not destroy or mutilate every item, in violation of their contracts. The Stambaughs transported the military property to their place of business in Mascoutah and sorted through the items to determine what could be converted to their own use or sold to others.

Brandon Schulte was a National Guardsman responsible for properly storing and disposing of military property at the Missouri Army National Guard facility in Jefferson City. The Stambaughs received military uniforms and other unauthorized, sensitive military property from Schulte, even though Schulte allegedly knew the Stambaughs were authorized to receive only scrap metal.

The indictment charges that Schulte understood he was required to follow specific procedures to dispose of sensitive military items, including uniforms. Such procedures are vital to national security, as terrorist groups overseas have previously acquired U.S. combat uniforms and used them to impersonate American soldiers, endangering American troops. Nevertheless, Schulte allegedly supplied the Stambaughs with thousands of pounds of military uniforms and other non-scrap military equipment. (Source)

U.S Army Reservist Sentenced To Prison For Participating In $1 Million+ Romance Scam / Money Laundering Scheme Using Dating Websites - July 9, 2021

Benjamin Alabie who was is a member of the United States Army Reserves, was sentenced yesterday to 40 months in prison for participating in a scheme to launder over $1 million in proceeds of romance fraud and business email compromise schemes perpetrated against dozens of victims.

Alabie laundered money for a scheme that trolled dating websites in order to steal money from the accounts of unsuspecting women.

From at least 2016 until 2018, Alabie participated in a scheme to launder the proceeds of frauds perpetrated against dozens of victims. Among other things, Alabie used false identities and false passports to open bank accounts, received or attempted to receive more than $2 million in fraud proceeds, withdrew tens of thousands of dollars of fraud proceeds in cash, and transferred more than $1 million of fraud proceeds to bank accounts controlled by co-conspirators in an effort to conceal the source of funds. (Source)

U.S. Army Green Beret Sentenced To Prison For Russian Espionage Conspiracy - May 14, 2021

Peter Debbins admitted to conspiring with agents of a Russian intelligence service. According to court documents, from December 1996 to January 2011, Debbins periodically visited Russia and met with Russian intelligence agents. In 1997, Debbins was assigned a code name by Russian intelligence agents and signed a statement attesting that he wanted to serve Russia.

From 1998 to 2005, Debbins served on active duty as an officer in the U.S. Army, serving in chemical units before being selected for the U.S. Army Special Forces. The Russian intelligence agents encouraged him to join and pursue a career in the Special Forces, which he did, where he served at the rank of Captain.

Over the course of the conspiracy, Debbins provided the Russian intelligence agents with information that he obtained as a member of the U.S. Army, including information about his chemical and Special Forces units.

In 2008, after leaving active duty service, Debbins disclosed to the Russian intelligence agents classified information about his previous activities while deployed with the Special Forces. Debbins also provided the Russian intelligence agents with the names of, and information about, a number of his former Special Forces team members so that the agents could evaluate whether to approach the team members to see if they would cooperate with the Russian intelligence service. (Source)

DoD Contractor Sentenced To Prison For Paying $100,000+ In Bribes To 2 U.S. Army Contracting Officials - January 15, 2021

John Winslett admitted that from 2011 to 2018, he paid over $100,000 worth of bribes to two U.S. Army contracting officials who worked at the Range at Schofield Barracks, in order to steer federal contracts worth at least $19 million to his employer, a government contractor. The bribes included cash, automobiles, and firearms. In return, the contracting officials used their positions to benefit Winslett's employer in securing U.S. Army contracts. (Source)

U.S. Army Reservist Sentenced To Prison For Role In $3 Million Romance Scam And Money Laundering Scheme - September 8, 2021

From at least in or about February 2018 through at least in or about September 2019, Joseph Asan and Charles Ogozy were members of the U.S. Army Reserves who participated in a scheme to commit fraud against victims across the United States, defraud banks, and launder over $3 million in fraud proceeds in bank accounts that they controlled.

The funds laundered by Asan and Ogozy were obtained primarily through (a) business email compromises, in which members of the scheme gained unauthorized access to or spoofed email accounts and impersonated employees of a company or third parties engaged in business with the company in order to fraudulently induce the victims to transfer money to bank accounts under the control of members of the scheme; and (b) romance scams, in which members of the scheme deluded unsuspecting older women and men into believing they were in a romantic relationship with a fake identity assumed by members of the scheme and used false pretenses to cause the victims to transfer money to bank accounts under the control of members of the scheme, including Asan and Ogozy. Notably, one of the victims of the defendants' scheme included a U.S. Marine Corps veteran's organization.

In order to launder over $3 million in proceeds from those fraud schemes, Asan and Ogozy opened several bank accounts in the names of fake businesses called Uxbridge Capital LLC, Renegade Logistics LLC, and Eldadoc Consulting LLC and received fraud proceeds in those bank accounts. Asan and Ogozy then laundered the fraud proceeds to each other and to other co-conspirators based in Nigeria. (Source)

U.S. Army National Guardsman & Government Employee Sentenced To Prison For Stealing And Selling $2.4 Million+ Worth Of Sensitive U.S. Military Equipment - November 19, 2020

A judge sentenced a former U.S. Property and Fiscal Office Program Analyst (Joseph Mora) and a former Texas Army National Guardsman (Cristal Avila) to prison for selling on the internet over $2.4 million in sensitive military equipment stolen from Camp Mabry in Austin, Texas.

From 2016 to 2019, Mora and Avila stole large quantities of government property, including scopes, infrared laser aiming devices and thermal night vision goggles, with an estimated value in excess of $2.4 million. Mora and Avila later sold the stolen goods on eBay and elsewhere. (Source)

U.S. Army National Guard Employee Sentenced To Prison For Role In $6 Million Government Contracting Fraud Scheme - November 2, 2020

From approximately 2009 through 2014, Dominic Caputo served as the Program Manager of the Power Division of the Oregon National Guard's OSMS at Camp Withycombe, an Oregon Military Department installation in Clackamas County. OSMS supports readiness and training of the U.S. Military by refurbishing out-of-service electronic equipment owned by the U.S. Department of Defense. In the event of an emergency or declaration of war, OSMS deploys refurbished equipment to other military bases or installations. During the time alleged in the Indictment and until 2015, OSMS was the only maintenance site in the United States capable of repairing and rebuilding certain models of electric generators and other small engines and parts in support of the federal military supply system.

In Fiscal Year 2014, Caputo billed the U.S. Army's Communications-Electronics Command (CECOM) more than $675,000 for the repair and rebuilding of John Deere Diesel Engines despite the work having not been performed. More than 60 of the engines had already been repaired and billed to CECOM in prior fiscal years. For those engines, Caputo directed Power Division employees to remove and replace original serial numbers and identifying engine plates from the engines to conceal the duplicate billing.

In June 2014, Caputo willingly and knowingly prepared a work order and run test data indicating that the falsified repair work on an engine had been performed. Caputo submitted this false information to CECOM. Caputo's employment with OSMS was terminated in November 2014 when his fraud was revealed. Despite the magnitude of the monetary losses, there was no evidence that Caputo engaged in the fraudulent conduct for his own financial enrichment. The fraud perpetuated an inefficient operation, and covered for defendant's own ineffective management.

Caputo billed for $6 million in repairs that were never done. (Source)

U.S. AIR FORCE (USAF)

USAF Civilian Employee Arrested For Stealing Top Secret Classified Information / Just Walked Out The Door Of Facility - August 13, 2024

On August 9, the FBI arrested Gohkan Gun, a Department of Defense civilian employee working with the U.S. Air Force who has been charged with mishandling classified materials, to include material classified as Top Secret. Gun is a dual-citizen of Turkey and the United States. At the time of his arrest he was waiting for a rideshare pickup at his Falls Church residence to take him to the airport for a 6 AM flight to Puerto Vallarta, Mexico. That didn't happen. The FBI arrived with a search warrant. Gun was arrested, and the FBI found hundreds of classified documents stacked in his dining room and in a backpack. In addition, the FBI found a document which catalog and listed his current U.S. government security clearances.

Gun began his work with the Air Force in mid-2023, just over a year ago, and apparently was a prolific hoarder of materials, having routinely printed documents to which he had access, often at the end of the work day. The investigation into Gun shows that 256 individual documents totaling more than 3400 pages were printed since his hire.

The exfiltration of documents by Gun was not sophisticated and perhaps would have been discovered had he been interrupted at the exit with a routine bag check for classified materials. Gun's M.O.? He rolled the printed documents into a wad and placed them in plastic shopping bags and carried them out the door. Some of the classified documents were printed and exfiltrated as recently as August 7, when it is believed Gun printed out at least 155 pages of Top Secret material which matched the titles of intelligence products on the top secret network. (Source)

U.SAF Employee Charged With Obstructing A Criminal Investigation Into Cause Of 2017 Military Plane Crash Killing 16 Service Members - July 10, 2024

On July 10, 2017, a United States Marine Corps KC-130 transport aircraft known as Yanky 72 crashed near Itta Bena, Mississippi, resulting in the death of fifteen Marines and one Navy Corpsman.

James Fisher is a former propulsion engineer with the C-130 program office at Robins Air Force Base, engaged in a pattern of conduct intended to avoid scrutiny for his past engineering decisions related to why the crash may have occurred. Specifically, the indictment alleges that Fisher knowingly concealed key engineering documents from criminal investigators and made materially false statements to criminal investigators about his past engineering decisions. (Source)

USAF Employee Charged for Unlawful Disclosure of Classified National Defense Information On Foreign Online Dating Website - March 4, 2024

David Slater worked in a classified space at USSTRATCOM and held a Top Secret security clearance from in or around August 2021 until in or around April 2022, after retiring as a Lieutenant Colonel from the U.S. Army.

Slater attended USSTRATCOM briefings regarding Russia's war against Ukraine that were classified up to TOP SECRET SENSITIVE COMPARTMENTED INFORMATION (TS//SCI). Slater then transmitted classified information that he learned from those briefings via the foreign online dating website's messaging platform to his co-conspirator, who claimed to be a female living in Ukraine on the foreign dating website. The co-conspirator regularly asked Slater to provide her with sensitive, non-public, closely held and classified information and called Slater in their messages her "secret informant love" and her "secret agent." In response to these requests, Slater indeed provided classified information to her, including regarding military targets and Russian military capabilities relating to Russia's invasion of Ukraine. (Source)

USAF Police Officer Convicted Of $150,000+ In COVID Unemployment Insurance Fraud During - March 5, 2024

Between April 2020 and June 2020, Treveon Miller submitted fraudulent claims in several states using his former name of Trevon Rodney. Miller told the state agencies that administer the unemployment insurance system that he was unemployed when he was an active-duty Air Force Police Officer the whole time. The claims were worth more than $150,000 and the money was put onto debit cards that were mailed to Miller. (Source)

USAF Disciplines 15 Members Over Leak of Classified Documents - December 11, 2023

The United States Air Force announced on Monday it has disciplined 15 members from a Massachusetts base following an inspector general's investigation into 21-year-old Airman 1st Class Jack Teixeira's alleged leak of national security documents on the social media platform Discord that was exposed earlier this year.

The inspector general's investigation was separate from the probe conducted by the Justice Department that resulted in Teixeira's arrest in April and subsequent indictment in June on six counts for the unauthorized disclosure of national defense information. Teixeira pleaded not guilty in June, remains behind bars and is still awaiting a trial date.

The Department of the Air Force released its report on Monday on the results of an Air Force Inspector General (IG) investigation that found individuals in Teixeira's unit, the 102nd Intelligence Wing, Otis Air National Guard Base, Massachusetts, "failed to take proper action after becoming aware of his intelligence-seeking activities."

Beginning on Sept. 7, Air National Guard leaders "initiated disciplinary and other administrative actions against 15 individuals, ranging in rank from E-5 to O-6, for dereliction in the performance of duties," the Air Force said.

The actions taken ranged from relieving personnel from their positions, including command positions, to non-judicial punishment under Article 15 of the Uniform Code of Military Justice. (Source)

USAF Base Director Sentenced To Prison For Conspiring To Pay Lobbyists, Consultants & Contractors $8.4 Million With Funds Fraudulently Obtained From United States Government - June 27, 2023

Beginning in 2004, Milton Boutte, who was then the Director of the Big Crow Program Office at Kirtland Air Force Base, conspired with others to pay lobbyists, consultants and contractors with funds fraudulently obtained from the United States.

Boutte conspired with George Lowe, a lobbyist, and Joe Diaz and Arturo Vargas, owners of Miratek and Vartek, two minority-owned small businesses that had sole-source contracts with the Big Crow Program Office. The conspirators disguised the nature of the claims for lobbying services provided by Lowe as well as other unauthorized subcontracts and expenditures. The Big Crow Program Office was not authorized to lobby or to expend appropriated funds for lobbying activities under the contracts.

Over the course of the conspiracy, Miratek and Vartek received approximately $8.4 million from the government. Of that amount, Boutte required those small businesses to pay nearly $4.1 million to lobbyists, consultants and contractors that Boutte had retained. Of that sum, Miratek and Vartek diverted more than $900,000 to Lowe, and another government contractor paid Lowe an additional $300,000. (Source)

USAF Sentenced To Prison For Retaining 300+ Classified Secret / Top Secret Documents - June 1, 2023

Robert L. Birchum (55, Tampa) to three years in federal prison for unlawfully possessing and retaining classified documents relating to the national defense of the United States. The court also ordered Birchum to pay a fine of $25,000.

Robert Birchum pleaded guilty to unlawfully possessing and retaining classified documents relating to the national defense of the United States on February. 21, 2023. Birchum previously served as a Lieutenant Colonel in the U.S. Air Force. During his 29-year career, Birchum served in various positions in intelligence, including those requiring him to work with classified intelligence information for the Joint Special Operations Command, the Special Operations Command, and the Office of the Director of National Intelligence. While on active duty, Birchum entered into several agreements with the United States regarding the protection and proper handling of classified information.

In 2017, however, law enforcement officers discovered that Birchum knowingly removed more than 300 classified files or documents, including more than 30 items marked Top Secret, from authorized locations. Birchum kept these classified materials in his home, his overseas officer's quarters, and a storage pod in his driveway. None of these locations were authorized for storage of classified national defense information. In particular, the criminal information charges that Birchum possessed two documents on a thumb drive found in his home that contained information relating to the National Security Agency's capabilities and methods of collection and targets' vulnerabilities. Both of these documents were classified as Top Secret/SCI, and their unauthorized release could be expected to cause exceptionally grave damage to the national security of the United States. (Source)

USAF Civilian Employee Sentenced To Prison For $2.3 Million+ Bribery And Government Contract Fraud Scheme Over 11 Years - April 25, 2023

Keith Seguin, a former civilian employee at Randolph Air Force Base in San Antonio, admitted to receiving millions of dollars in bribes in connection with a government contract fraud scheme that spanned more than a decade and impacted hundreds of millions of dollars in contract awards.

According to formal charges, the QuantaDyn Corporation, a software engineering company based in Ashburn, Virginia; its owner, David Bolduc; Rubens Lima and Seguin all conspired to secure government contracts.

Seguin used his position to steer lucrative contracts and sub-contracts to QuantaDyn for aircraft and close-air-support training simulators. Seguin, who was intimately involved in the government contracting process, leaked confidential competitor proposals to a prime contractor who would then subcontract the work to QuantaDyn. He also leaked confidential government budget information to prime contractors and to QuantaDyn, enabling them to maximize profits at government expense. Seguin admitted to accepting more than $2.3 million in bribes from Bolduc and QuantaDyn from 2007 to 2018. (Source)

2 Former Managers Working For USAF Private Housing Contractor Sentenced To Probation For Defrauding Air Force Out $3.5 Million - September 13, 2022

Stacy Cabrera, who managed Balfour Beatty Communities-owned housing at Lackland Air Force Base, Texas, and Rick Cunefare, who was a regional manager at Balfour Beatty, were both sentenced Thursday in the U.S. District Court for Washington, D.C., according to court records.

Both Cabrera and Cunefare pleaded guilty in 2021 to charges stemming from a scheme in which Balfour Beatty was accused of manipulating maintenance records to obtain performance bonuses from the military while covering up unsafe housing conditions from 2013 to 2019.

The company itself pleaded guilty last year to the scheme to defraud the Army, Air Force and Navy, and agreed to pay $65 million in fines and restitution.

Cunefare, who pleaded guilty to major fraud, was responsible for reviewing and approving the maintenance reports from Lackland, as well as Travis, Vandenberg, Tinker and Fairchild Air Force bases. according to the Justice Department. Cabrera, who pleaded guilty to conspiracy to commit wire fraud, was accused of personally falsifying maintenance reports.

Together, their actions made Balfour Beatty about $3.5 million the company didn't earn, the Justice Department said in a sentencing memo. Still, because they were both "low- and mid-level managers with minimal financial incentive to commit fraud," prosecutors sought lenient sentences.

Cabrera has said she was pressured by her superiors to fake the reports, but has also expressed regret for her actions. (Source)

USAF National Guardsman Charged In Murder-For-Hire Scheme / Needed Money - April 14, 2023

Josiah Garcia needed money to support his family and in mid-February began searching online for contract mercenary jobs and came across the website www.rentahitman.com. Originally created in 2005 to advertise a cyber security startup company, the company failed and over the next decade it received many inquiries about murder-for-hire services. The website's administrator then converted the website to a parody site that contains false testimonials from those who have purported to use hit man services, and an intake form where people can request services. The website also has an option for someone to apply to work as a hired killer.

Garcia submitted an employment inquiry indicating that he was interested in obtaining employment as a hit man. Garcia followed up on this initial request and submitted other identification documents and a resume, indicating he was an expert marksman and employed in the Air National Guard since July 2021. The resume also indicated that Garcia was nicknamed "Reaper" which was earned from military experience and marksmanship. Garcia continued to follow up with the website administrator indicating that he wanted to go to work as soon as possible.

An FBI undercover agent then began communicating with Garcia who subsequently agreed to kill an individual for $5,000. On Wednesday, Garcia met the undercover agent at a park in Hendersonville, Tennessee, and was provided with a target packet of a fictional individual, which included photographs and other information about the individual to be killed, and a down payment of $2,500. After agreeing to the terms of the murder arrangement, Garcia asked the agent if he needed to provide a photograph of the dead body. Garcia was then arrested by FBI agents, who in a subsequent search of his home, recovered an AR style rifle. (Source)

USAF Contracting Specialist Sentenced To Prison For Accepting $47,000 In Bribes For Confidential Bidding Information On $8.2 Million Worth Of Contracts - November 9, 2022

Brian Nash is a former U.S. Air Force Contract Specialist who was assigned to Joint Base Elmendorf Richardson (JBER).

Nash agreed to accept more than $460,000 in bribe payments in 2019 from a government contractor, Ryan Dalbec, who, along with his wife, Riahnna Nadem, owned a construction company called Best Choice Construction LLC.

In exchange, Nash provided Dalbec and Nadem with confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson AFB and JBER, which helped Best Choice win some of the contracts, including a construction contract related to the F-35 aircraft program at Eielson Air Force Base and contracts to perform construction and related services at JBER.

At the time Nash was caught he had received approximately $47,000 of the agreed upon bribe payments, much of which he laundered through family members to conceal the nature and source of the funds. The defendants committed multiple overt acts in furtherance of the bribery conspiracy, and between March and October 2019 Dalbec, Nadem and Nash laundered payments and proceeds from the bribery scheme to conceal their unlawful activities. (Source)

DoD Construction Contractor Owner Sentenced To Prison For Agreeing To Pay $460,000+ In Bribes To USAF Contracting Official - December 8, 2022

Ryan Dalbec is the owner of Best Choice Construction LLC (Best Choice).

Dalbec agreed to pay over $460,000 in bribes to former U.S. Air Force Contracting Official, Brian Nash, in exchange for confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson Air Force Base and Joint Base Elmendorf-Richardson (JBER).

The confidential bidding information Nash provided helped Dalbec and Best Choice win some of those contracts, including a $6,850,000 construction contract related to the F-35 aircraft program at Eielson Air Force Base. Dalbec and his wife, Raihana Nadem, also helped Nash launder the bribery proceeds through family members and third-party bank accounts to conceal the nature and source of the funds.

Nash was previously sentenced to serve 30 months imprisonment and ordered to forfeit $47,000 in unlawful gains. (Source)

2 Former USAF Daycare Employees Charged For Cruelty To Children, Simple Battery, Failure to Report Suspected Child Abuse - October 12, 2022

The indictment alleges a variety of felony cruelty to children actions committed by Zhanay Flynn and Antanesha Fritz, two former Robins Air Force Base daycare employees, during Jan. and Feb. 2021.

The charges allege various forms of abuse, to include striking children, causing children to fight each other, forcing children to hit one another, spraying children in the face with a cleaning liquid, seizing and shaking a child while threatening to strike them, striking a child in the head with a book, kicking a child into a wall, and stepping on and applying weight to a child's leg. Flynn and Fritz are also accused of committing simple battery against children, with the indictment alleging that they lifted a cot with a child sleeping on it, causing the child to fall on the ground, struck a toy out of a child's hand and then forced the child into a small enclosure, and sprayed two children in the head and face with a cleaning solution. Latona Lambert the former daycare director, Flynn and Fritz are each charged with one count of failing to report suspected child abuse when they did not notify the proper authorities of the abuse after allegedly witnessing it or having reason to suspect that abuse was occurring.

Zhanay Flynn is charged with 18 counts of cruelty to children in the first degree, six counts of cruelty to children in the second degree, three counts of simple battery and one count of failure to report suspected child abuse.

Antanesha Fritz is charged with 18 counts of cruelty to children in the first degree, six counts of cruelty to children in the second degree, three counts of simple battery and one count of failure to report suspected child abuse.

Latona Lambert is charged with one count of failure to report suspected child abuse. (Source)

USAF Employee Sentenced Prison For Using Government Credit Card To Obtain $1.1 Million+ Of Cash Advances For Personal Use - November 29, 2021

From January 2003 to February 2018, Eddie Ray Johnson Johnson was a civilian Air Force employee, most recently as a travel coordinator in the Secretary of the Air Force, Office of Legislative Liaison, where he planned congressional travel and reviewed and approved accounting packages submitted by trip escorts, among other duties.

Johnson admitted that from March 2014 through September 2017, he used his government-issued travel credit card to obtain more than $1.1 million in cash advances, at least $774,000 of which he diverted to his own personal use. (Source)

USAF Contractor Sentenced To Prison For Taking 2,500 Pages Of Classified Information - September 21, 2021

Izaak Kemp was employed as a contractor at the Air Force Research Laboratory (AFRL) from July 2016 to May 2019, and later as a contractor at the U.S. Air Force National Air and Space Intelligence Center (NASIC).

While working at AFRL and NASIC, both located on Wright-Patterson Air Force Base in Fairborn, Kemp had Top Secret security clearance.

Despite having training on various occasions on how to safeguard classified material, Kemp took 112 classified documents and retained them at his home.

Law enforcement discovered the more than 100 documents, which contained approximately 2,500 pages of material classified at the SECRET level, while executing a search warrant at Kemp's home on May 25, 2019. (Source)

USAF Base Major / Nurse Sentenced To Prison For Receiving $73,000+ In Kickbacks For TRICARE Prescription Drug Scheme - August 10, 2020

Romeatruis Moss solicited and received $73,823.06 in return for referring prescriptions for members of the U.S. military to compounding pharmacies that were reimbursed by TRICARE, a health insurance program for military members. Because of resulting cost increases and infringement on patient choice, it is a crime to solicit or receive payments for referrals to health care providers for an item or service that could be paid, in whole or in part, by a federal health care program.

Moss admitted that while she was employed in the medical unit at Vance AFB, she gave military members pre-printed prescription pads and induced them to ask their doctors for specific compounded drugs. Moss admitted she then sent the prescriptions or caused them to be sent to specific pharmacies. Moss admitted she was paid a kickback that was a percentage of the gross reimbursement the pharmacies received from TRICARE for filling the prescriptions. (Source)

U.S. NAVY (USN)

USN Petty Officer Sentenced To Prison For Stealing $856,000+ Of Military Gear And Selling It - November 21, 2024

Richard Allen was sentenced to prison for orchestrating a conspiracy that stole more than $850,000 worth of military gear earmarked for fellow Navy members, and then sold the goods to high bidders.

While stationed at Naval Weapons Station Yorktown-Cheatham Annex, in Williamsburg, VA, Richard Allen and others repeatedly broke into a warehouse on the Navy base that held U.S. Navy gear, including working uniforms, winter gear, flame retardant shirts and pants, soft body armor, goggles, infrared flag patches, Navy SEAL Trident insignia, and Small Arms Protective Insert plates.

Paying Customers

China, Russia, South Korea, Hong Kong, Kazakhstan, Bahrain, Vietnam, Ukraine, Indonesia, Japan, Malaysia, Thailand, Germany, Singapore, Taiwan, the Czech Republic, Poland, Australia, New Zealand, France, Spain, Ireland, Portugal, Italy, Greece, the United Kingdom, Norway, Switzerland, Finland, Turkey, Austria, Slovenia, Croatia, Hungary, Slovakia, Belgium, Brazil, Philippines, Denmark, the Netherlands, Sweden, Uruguay, Chile, Estonia, Malta, Lithuania, Bermuda, and Canada, and conspirators assisted him in also distributing to Argentina, Luxembourg, Latvia, Belarus, Denmark, and Martinique.

Allen and his co-conspirators stole $856,433 worth of Navy gear and supplies, storing the items in various locations, including in Rhode Island. Allen and others then identified bulk-sale domestic and international customers for the stolen goods and arranged for delivery either in person or via commercial shipping. Payment for the stolen goods was frequently made and received via PayPal, including dozens of payments made from an account in China. The proceeds were transferred to co-conspirators bank accounts, including Allen's, in increments of less than $10,000, in an effort to avoid bank reporting requirements. (Source)

USN Contractor Executive Charged For Bribing U.S. Naval Information Warfare Center Employee For $50 Million Of Contracts - October 30, 2024

Mark Larseng (Cask Technologies, LLC Company Executive) and his subordinates at Cask gave former Naval Information Warfare Center employee James Soriano various things of value, including expensive meals, golf outings, and full-time jobs for Soriano's close family friend and immediate family member. At the time of the conspiracy, Larsen was the director, and later the managing director, vice president, and executive vice president of Cask with offices in San Diego and Stafford, Virginia.

In return, Soriano took official action to benefit Cask, such as steering non-competitive small business contracts to Cask and its "family" of companies; allowing Larsen and other Cask employees to draft procurement documents for various contracting efforts, including competitive procurements; and allowing Larsen and others to "ghost write" emails, official government correspondence, and performance evaluations for Soriano's signature, all to benefit Cask and others in its "family" of companies.

Soriano also agreed in an email exchange to "create & award" a $50 million supposedly competitive contract for services to Cask. Soriano then allowed Cask to draft the contract requirements and the price the government was expected to pay, and took other actions to ensure that Cask was awarded the "competitive" contract. (Source)

USN Civilian Employee Pleads Guilty To Bribery Scheme Involving Government Contracts - June 12, 2024

James Soriano is a former civilian employee of the San Diego based Naval Information Warfare Center (NIWC).

Soriano pleaded guilty to multiple bribery conspiracies, admitting that while he was a public official at NIWC, he accepted hundreds of thousands of dollars from defense contractors in the form of free meals, tickets to premier sporting events, jobs for family and friends, and other things, in exchange for helping those contractors win and maintain hundreds of millions of dollars in government contracts.

According to Soriano's plea agreement, from approximately March 2016 through at least October 2019, Soriano and a coworker, Dawnell Parker, received bribes from Philip Flores, the President and CEO of Intellipeak Solutions, Inc., a defense contractor headquartered in Fredericksburg, Virginia. Soriano also admitted that from approximately May 2015 through at least October 2019, he and Parker separately received bribes from another defense contractor, with offices in San Diego and Stafford, Virginia, who also gave him things of value, such as expensive meals, a job for his wife, and rounds of golf at private country clubs.

Further, according to Soriano's plea agreement, from approximately June 2014 through at least October 2019, Soriano received bribes from Russell Thurston, the Vice President of Cambridge International Systems, Inc., a defense contractor headquartered in Arlington, Virginia. In return for these bribes, Soriano used various methods to steer contracts to these defense contractors and kept his contracting activities hidden from the Naval Information Warfare Center.

According to Soriano's plea agreement, the defense contractors acting through their presidents, officers, and employees gave various things of value to Soriano, including dinners at Ruth's Chris, Island Prime, and Providence; tickets to the 2018 MLB All-Star Game, 2018 World Series, and 2019 Superbowl; and jobs for Soriano's family and friends, including a member of Soriano's family and Soriano's family friend, Liberty Gutierrez, who was giving Soriano $2,000 a month from her salary at one of the companies working under a defense contract. (Source)

USN Officer Sentenced To Prison For Afghan Visa Bribery Scheme - October 28, 2024

Cmdr. Jeromy Pittmann, a U.S. Navy Reserve officer was sentenced to more than two years in prison for his role in a years-long bribery scheme involving Special Immigrant Visas (SIVs) for Afghan citizens.

Pittmann served as a civil engineer corps officer who deployed to Afghanistan with NATO Special Operations Command.

Pittmann received several thousands of dollars in bribes from Afghan nationals in exchange for drafting, submitting and verifying fraudulent letters of recommendation for Afghan citizens who applied for SIVs with the State Department.

To avoid detection, Pittmann received the bribe money through an intermediary and created false invoices showing that he was receiving the funds for legitimate work unrelated to his military service.

The State Department offers a limited number of SIVs to enter the United States. Pittman signed more than 20 letters stating he knew and supervised Afghan national applicants while they worked as translators in support of the U.S. military and NATO. (Source)

USN Chief Petty Officer Pleads Guilty To Stealing & Selling $164,000+ Of Military Equipment - October 28, 2024

Shawn Crowell was assigned to Helicopter Sea Combat Wing Atlantic at Naval Station Norfolk from December 2022 to September 2024. Crowell had access to and was responsible for the inspection and inventorying of the military equipment belonging to the Command.

From at least January through June 2023, Crowell stole numerous government items, including seven sets of Night Vision Goggles (NVGs, or NODs), two Matbock Tarsier Eclipse lenses, and eight NVG battery packs. The value of the items stolen by Crowell was at least $164,646.

Between February and May 2023, Crowell used online advertisements to sell five sets of the stolen NVGs to third-party purchasers for $19,947. On March 8, 2023, Crowell listed for sale the two Matbock Tarsier Eclipse lenses, which are regulated by the International Trafficking in Arms Regulations (ITAR). Crowell sold the stolen lenses for $300. On April 1, 2023, Crowell sold the eight NVG battery packs for $500. (Source)

USN Shipyard Contractor Sentenced To Prison For Stealing Almost $600,000 Worth Of Computer Equipment From Navy - July 10, 2024

Ernesto Saldivar was a civilian contractor at General Dynamics who was employed as part of the shipyard's modernization efforts. ,

From November 2022 to August 2023, Saldivar stole hundreds of military hard drives and laptops from declassified areas on ships undergoing maintenance. Saldivar then sold the stolen items on eBay. Two of the hard drives he stole contained classified military communications. The affected ships included the USS Pinckney, USS Curtis Wilbur and USS Spruance. The total value of the stolen computer equipment – including two laptops, two programmer units, four DC-DC converters, 18 power converters, and 302 hard drives – totaled $596,997.53.

During the investigation of the missing hard drives, the U.S. Army Criminal Investigation Laboratory conducted a forensic analysis on fingerprints left inside the empty hard drive trays. These interior areas of the hard drive trays could only be touched after a hard drive was removed.

The prints belonged to Saldivar. Naval Criminal Investigative Service agents also traced eBay listings of some of the stolen equipment to Saldivar. And, during a court-authorized search of Saldivar's home on August 25, 2023, NCIS agents recovered 120 of the missing hard drives, a Panasonic Toughbook laptop from the USS Pinckney with software from Integrated Voice Communications System (IVCS), several DC-DC converters traceable to the USS Pinckney, a BPM Microsystems 1410 taken from the Curtis Wilbur, and a BPM Microsystems 1710 Universal Device Programmer matching the serial number of an inventoried loss, all stored haphazardly in a shed on Saldivar's property. (Source)

USN Admiral (Now Retired) & Business Executives Arrested In Connection With Alleged Bribery Scheme - May 31, 2024

From 2020 to 2022, Robert Burke was a four-star Admiral who oversaw Naval operations in Europe, Russia, and most of Africa, and commanded thousands of civilian and military personnel.

Yongchul "Charlie" Kim and Meghan Messenger were the co-CEOs of a company (Company A) that provided a workforce training pilot program to a small component of the Navy from August 2018 through July 2019. The Navy terminated a contract with Company A in late 2019 and directed Company A not to contact Burke.

Despite the Navy's instructions, Kim and Messenger then allegedly met with Burke in Washington, D.C., in July 2021, in an effort to reestablish Company A's business relationship with the Navy. At the meeting, the charged defendants allegedly agreed that Burke would use his position as a Navy Admiral to steer a sole-source contract to Company A in exchange for future employment at the company. They allegedly further agreed that Burke would use his official position to influence other Navy officers to award another contract to Company A to train a large portion of the Navy with a value Kim allegedly estimated to be "triple digit millions."

In furtherance of the conspiracy, in December 2021, Burke allegedly ordered his staff to award a $355,000 contract to Company A to train personnel under Burke's command in Italy and Spain. Company A performed the training in January 2022. Thereafter, Burke allegedly promoted Company A in a failed effort to convince a senior Navy Admiral to award another contract to Company A. To conceal the scheme, Burke allegedly made several false and misleading statements to the Navy, including by creating the false appearance that Burke played no role in issuing the contract and falsely implying that Company A's employment discussions with Burke only began months after the contract was awarded.

In October 2022, Burke began working at Company A at a yearly starting salary of $500,000 and a grant of 100,000 stock options.

Burke, Kim, and Messenger are each charged with conspiracy to commit bribery and bribery. Burke is also charged with performing acts affecting a personal financial interest and concealing material facts from the United States. If convicted, Burke faces a maximum penalty of 30 years in prison, and Kim and Messenger each face a maximum penalty of 20 years in prison. (Source)

USN Chief Petty Officer Found Guilty For Passing Classified Information To A Foreign Government - April 21, 2024

Chief Petty Officer Fire Controlman Bryce Pedicini, a sailor assigned to a guided-missile destroyer based in Japan, has been found guility of espionage for and passing classified information to a foreign government contact.

Prosecutors contended in a March 15 filing that an unnamed foreign government employee contacted Pedicini via Facebook Messenger and stated he or she was a defense researcher who offered him money in exchange for information about the U.S. military capabilities and strategies in the specific region.

Starting in November 2022 and continuing into May 2023 in the Hampton Roads, Va., area, the government alleged, Pedicini sent various documents through Facebook Messenger and other electronic means, including Signal and Telegram, and in May 2023 sent photographs he accessed via a classified SIPR terminal. At one point, that contact sent him a reportedly "secret" document "as an example" of documents they sought from him, a point his defense attorneys later argued was "inflammatory evidence" but not a wrongful act.

In a filing earlier this month, government prosecutors alleged the chief had received money paid via PayPal to his credit union account. "In exchange for national defense information, the accused sought and received monetary payment from Individual #1," the document stated

Pedicini had also been charged with failing to report foreign contacts to his chain of command, failing to report solicitation of classified information, taking a personal device into a secure room, and transporting classified information. (Source)

USN Navy Sailor Sentenced To Prison For Transmitting Sensitive U.S. Military Information To Chinese Intelligence Officer / Received 14 Bribe Payments - January 8, 2024

Thomas Zhao pleaded guilty in October 2023 to one count of conspiracy and one count of receiving a bribe in violation of his official duties.

Zhao, who was stationed at Naval Base Ventura County in Port Hueneme, held a U.S. security government clearance and underwent routine trainings on efforts by hostile nation states to acquire sensitive information.

Between August 2021 and at least May 2023, Zhao received at least $14,866 in 14 separate bribe payments from the intelligence officer, who directed Zhao to surreptitious collect and transmit sensitive U.S. military information and offered to pay Zhao bonuses for controlled and classified information.

In exchange for the illicit payments, Zhao repeatedly entered restricted military and naval installations to secretly collect non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao used encrypted communications to transmit that sensitive, non-public information to the intelligence officer. Zhao transmitted plans for a large-scale maritime training exercise in the Pacific theatre, operational orders, and electrical diagrams and blueprints for a Ground/Air Task Oriented Radar system located in Okinawa, Japan. (Source)

USN Service Member Sentenced To Prison For $2 Million Insurance Fraud Scheme - October 17, 2023

Christopher Toups, who at the time of his crimes was a Chief Petty Officer in the U.S. Navy, was sentenced in federal court to 30 months in prison after admitting that he and others defrauded an insurance program meant to compensate service members who suffer serious and debilitating injuries while on active duty.

Participants in the scheme obtained approximately $2 Million in payments from fraudulent claims submitted to Traumatic Servicemembers Group Life Insurance Program, or TSGLI, and Toups personally obtained about $400,000. TSGLI was funded by service members and the Department of the Navy.

Toups admitted that from 2012 to at least December 2015, he conspired with his then-spouse Kelene McGrath, Navy Dr. Michael Villarroel, and others to obtain money from the United States by making claims for life insurance payments based on exaggerated or fake injuries and disabilities. (Source)

USN IT Manager Sentenced To Prison For Hacking a Computer Database, Stealing 9,000 People's Identities & Selling Information For $160,000 In Bitcoin - October 16, 2023

Marquis Hooper is a former Navy IT Manager.

In August 2018, Hooper opened an online account with a company that runs a database containing the PII for millions of people. The company restricts access to the database to businesses and government agencies that have a demonstrated, lawful need for the PII. Hooper, however, opened his database account by falsely representing to the company that the Navy needed him to perform background checks.

After Hooper opened his database account, he added his wife and co-defendant, Natasha Chalk, to the account. They then stole over 9,000 people's PII and sold it to other individuals on the dark web for $160,000 in bitcoin. At least some of the individuals to whom Hooper and Chalk sold the PII used it to commit further crimes.

In December 2018, Hooper's database account was closed for suspected fraud. Thereafter, Hooper, Chalk, and an unindicted co-conspirator tried to regain access to the database. Hooper instructed the unindicted co-conspirator to open a new database account by representing that the Navy needed him to perform background checks just like Hooper had done. Hooper offered to pay the unindicted co-conspirator $2,500 for each month that the database account was opened. The unindicted co-conspirator submitted an application to open the database account and the company told him that a supply officer had to sign the contract.

Hooper then sent the unindicted co-conspirator multiple documents falsely identifying an identity theft victim as the supposed Naval supply officer. These documents included a false contract, a fake driver's license for the identity theft victim, and a forged letter purporting to be from a commanding officer in the Navy. The unindicted co-conspirator submitted the fake documents to the company, but the company decided not to open the new database account. (Source)

2 USN Navy Sailors Arrested For National Security Reasons Relating To China - August 3, 2023

The Department of Justice arrested two U.S. Navy sailors on national security charges relating to China. It is unclear whether the two cases are connected in any way.

The first sailor, a 22 year old Petty Officer assigned to a Navy vessel in San Diego. He was arrested on an espionage charge relating to a conspiracy to share intelligence with a Chinese official. The Petty Officer who served as a Construction Engineer, is charged with conspiring with a PRC Intelligence Officer to collect and transmit sensitive military information about naval operations. The Petty Officer allegedly accepted bribes and gave the PRC intelligence officer photographs and videos of military exercise plans, operational orders and electrical systems.

The second sailor, based near Los Angeles, is charged with conspiracy and receipt of a bribe from a Chinese official. The sailor faces charges for espionage and for violating export control laws, for collecting and transmitting sensitive national defense information at the direction of a PRC Intelligence Officer.

As tasked by the PRC Intelligence Officer, the sailor allegedly transmitted or attempted to transmit more than 50 manuals and other documents containing technical and mechanical data about naval amphibious assault ships Several of these materials were allegedly marked with export control warnings and contained details about the power structure, weapons systems and damage control aboard those ships. (Source)

USN Nuclear Engineer & Wife Sentenced To Prison For Espionage Related Offenses - November 9, 2022

Jonathan Toebbe of Annapolis, was sentenced today to 19 years and 4 months of incarceration and fined $45,700. His wife, Diana Toebbe was sentenced to 21 years and 10 months of incarceration and fined $50,000. The Toebbes pleaded guilty to the conspiracy in August 2022.

Jonathan Toebbe was an employee of the Department of the Navy who served as a Nuclear Engineer and was assigned to the Naval Nuclear Propulsion Program. He held an active national security clearance through the Department of Defense, giving him access to "Restricted Data" within the meaning of the Atomic Energy Act. Restricted Data concerns design, manufacture or utilization of atomic weapons, or production of Special Nuclear Material (SNM), or use of SNM in the production of energy, such as naval reactors. Jonathan Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships.

Toebbe sent a package to a foreign government, listing a return address in Pittsburgh, Pennsylvania, containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was really an undercover FBI agent. Toebbe continued this correspondence for several months, which led to an agreement to sell Restricted Data in exchange for thousands of dollars in cryptocurrency.

On June 8, 2021, the undercover agent sent $10,000 in cryptocurrency to Jonathan Toebbe as "good faith" payment. Shortly afterwards, on June 26, Jonathan Toebbe serviced a dead drop by placing an SD card, which was concealed within half a peanut butter sandwich and contained military sensitive design elements relating to submarine nuclear reactors, at a pre-arranged location. After retrieving the SD card, the undercover agent sent Jonathan Toebbe a $20,000 cryptocurrency payment. In return, Jonathan Toebbe emailed the undercover agent a decryption key for the SD Card. A review of the SD card revealed that it contained Restricted Data related to submarine nuclear reactors. On Aug. 28, Jonathan Toebbe made another "dead drop" of an SD card in eastern Virginia, this time concealing the card in a chewing gum package. After making a payment to Jonathan Toebbe of $70,000 in cryptocurrency, the FBI received a decryption key for the card. It, too, contained Restricted Data related to submarine nuclear reactors. The FBI arrested Jonathan Toebbe and his wife on Oct. 9, after he placed yet another SD card at a pre-arranged "dead drop" at a second location in West Virginia. (Source)

Senior USN Employee Convicted For Bribery (Cash, Travel, Prostitutes, Etc.) - August 24, 2022

Fernando Monroy is the former Director of Operations of the U.S. Navy's Military Sealift Command Office in Busan, South Korea.

Monroy engaged in a conspiracy to commit bribery with the owner of DK Marine, a South Korea-based company that provided services to the U.S. Navy, and a former civilian U.S. Navy cargo ship captain. Evidence at trial proved that Monroy conspired to unlawfully provide services for the Navy ship, captained by one of Monroy's co-conspirators, during a December 2013 port visit in Chinhae, South Korea.

Monroy provided a co-conspirator with confidential and other proprietary, internal U.S. Navy information. In exchange for the steering of business and the provision of such information, the co-conspirator paid bribes to Monroy, including cash, personal travel expenses, meals and alcoholic beverages, and the services of prostitutes. Monroy also repeatedly lied to special agents of the Defense Criminal Investigative Service (DCIS) and Naval Criminal Investigative Service (NCIS) during a voluntary interview in July 2019. (Source)

Naval Criminal Investigative Service (NCIS) Agent Sentenced To Prison For Corruption Related To Relationship With Syrian Businessman - December 15, 2022

A 49 year-old former Special Agent with NCIS has been sent to prison following her conviction of obstructing justice, making false statements and accepting money and gifts for official acts.

Leatrice Daniels was a veteran NCIS special agent working in Dubai, United Arab Emirates. There, she met Nadal Diya, a Syrian businessman living in Dubai looking for help in securing a visa to the United States. At that time, Diya was the target of several federal investigations.

At trial, the jury heard from 16 government witnesses, which included numerous agents and Diya himself. Testimony revealed that in 2017, Daniels used her position to get certain benefits from Diya in exchange for providing information to him about his visa status. The gifts included an expensive birthday party at Diya's home, approximately $1,400 in cash and the promise of a job for her son in Diya's company.

The relationship with Diya eventually became sexual. During that relationship, she revealed he was a target of an FBI counterterrorism investigation, information that was classified at the time. She also told him that if he came to the United States, he would likely be arrested.

In late December 2017, federal agents had questioned Daniels about Diya. However, she failed to disclose her intimate relationship with him, the gifts he had given her, the job he offered her son and the classified information she provided.

Following the interview, she also visited with Diya and coached him on what to say in a subsequent interview.

Several months later in May 2018, she left Dubai for Hawaii for a highly sensitive and coveted job. However, she soon learned she would not get the new position. It was only then she confessed to superiors and investigators about her illicit relationship, the monies, party and gifts she had received and the classified information she had previously revealed.

Daniels testified in her own defense at trial. She claimed, among other things, that the classified information she revealed to Diya was public information. She further attempted to convince the jury she did not have a duty to reveal any of the details of her personal relationship with Diya nor her disclosures to him. The jury did not believe her claims and found her guilty. (Source)

Former Metallurgist Lab Director Sentenced To Prison To Falsifying Test Results For Strength Of USN Submarines Hulls / Navy Has Spent $14 Million To Esnure Submarines Are Safe - February 14, 2022

The former Director of Metallurgy (Elaine Thomas) at Bradken Inc. was sentenced to prison, and a $50,000 fine, for falsifying test results that measure the strength and toughness of steel that Bradken sold for installation in U.S. Navy submarines.

Thomas falsified test results to hide the fact that the steel had failed the tests. Thomas falsified results for over 240 productions of steel, which represents about half the castings Bradken produced for the Navy.

According to records filed in the case, Bradken is the U.S. Navy's leading supplier of high-yield steel castings for naval submarines. Bradken's Tacoma foundry produces castings that prime contractors use to fabricate submarine hulls. The Navy requires that the steel meets certain standards for strength and toughness to ensure that it does not fail under certain circumstances, such as a collision. For 30 years, the Tacoma foundry (which was previously known as Atlas, and acquired by Bradken in 2008), produced castings, many of which had failed lab tests and did not meet the Navy's standards.

Court filings indicate there is no evidence that Bradken's management was aware of the fraud until May 2017. At that time, a lab employee discovered that test cards had been altered and that other discrepancies existed in Bradken's records. In April 2020, Bradken entered into a deferred prosecution agreement, accepting responsibility for the offense and agreeing to take remedial measures. Bradken also entered into a civil settlement, paying $10,896,924 to resolve allegations that the foundry produced and sold substandard steel components for installation on U.S. Navy submarines.

The Navy has taken extensive steps to ensure the safe operation of 30 affected submarines. Those measures will result in increased costs and maintenance as some of the substandard parts are monitored. To date, the Navy says it has spent nearly $14 million including 50,000 hours of engineering work to assess the parts and risk to the submarines. (Source)

USN Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy - December 21, 2021

Ivy Wang is a former U.S. Navy sailor who was a Logistics Specialist First Class assigned to the Naval Special Warfare Command. Ivy Wang conspired with her husband Eric Wang, to illegally export sensitive military equipment to China for profit.

Eric Wang pleaded guilty that he illegally sold export-controlled U.S. military equipment to China through his on-line business and that he enlisted his wife to use her Navy position to purchase the equipment for resale. Eric Wang also admitted that he maintained a warehouse in China to house the military equipment, travelled back and forth frequently, and had connections to buyers in China. (Source)

USN Intelligence Software Engineer Pleads Guilty To Operating An Illegal Steroid Manufacturing & Distribution Business For 8 Years - October 27, 2021

Possessed More Than 8,000 Doses of Illegal Steroids and More Than 160 Firearms

From 2013 to April 2021, Justin Best operated an illegal steroid manufacturing business from his Laurel, Maryland residence and conspired with others to distribute and possess with the intent to distribute, home manufactured steroids throughout the United States.

Law enforcement executed a search warrant at Best's Laurel, Maryland residence. Officers located and seized 8,500 units of controlled substances used in manufacturing steroids, including two 2,000-milliliter jars of testosterone cypionate, 198 pills of oxandrolone, 114 pills of stanozolol, 61 pills of oxymetholone, nine 10-milliliter vials of testosterone enanthate, one 10-milliliter vial of testosterone phenylpropionate, syringes, and packaging and mailing materials.

In addition to precious metals, collectable coins, and $6,127 in cash, officers recovered approximately 167 firearms consisting of 120 handguns, 39 rifles, seven shotguns, and 25 silencers. Officers also seized hundreds of thousands of rounds of ammunition, as well as 277 firearm magazines and 18 sets of firearm accessories from Best's garage. Best agreed that the seized firearms, silencers, ammunition, magazines and firearm accessories were purchased with proceeds of his manufacturing and distribution of controlled substances. (Source)

USN Active Duty Sailor And His Former Navy Colleague Charged With Conspiring To Traffic Guns - August 31, 2021

Elijah Boykin, an active-duty U.S. Navy Sailor, and Elijah Keashon Barnes have been indicted for unlawfully obtaining and transporting dozens of firearms that were later used in New Jersey-area crimes. Boykin and Barnes served together in the U.S. Navy until June 2020, when Barnes was discharged following his confinement for repeated violations of military law.

Between April 2020 and August 2020, Elijah Isaiah Boykin purchased more than two dozen firearms from federally licensed firearms dealers in Georgia and Virginia. The total purchase price exceeded $17,000 and was spread over eight transactions. On each occasion, Boykin signed paperwork stating that he was the actual purchaser of the guns but paid using a credit card belonging to co-defendant Elijah Keashon Barnes.

Local law enforcement in and around Newark, New Jersey began to recover Boykin's firearms shortly after they were purchased. One pistol was recovered in October 2020, when police officers in Newark conducted a traffic stop and arrested Barnes, who was wanted on a Virginia warrant for domestic assault and battery. The pistol was found in Barnes's car. A few months later, Newark police officers recovered another gun that Boykin purchased. Forensic testing linked that second firearm to three separate shootings in Newark, including a violent mugging during which a victim was shot multiple times in the right leg. (Source)

Former DoD Official Pleads Guilty To Taking $37,00 In Cash Bribes To Aid USN Contractor's Request For $6.4 Million From DoD - July 13, 2021

In 2014 and 2015 Nizar Farhat was on assigned temporary duty at the United States Navy Base Camp Lemonnier in Djibouti, Africa where he oversaw a private company's $15 million contract to construct an aircraft hangar and a telecommunications facility. After the projects were completed, the company submitted to the Defense Department Requests for Equitable Adjustment (REAs) that sought $6.43 million in additional payments.

Farhat admitted that, on four separate occasions between December 2015 and October 2017, he met with representatives of the contracting company at hotels in Las Vegas and Palm Springs. During those meetings, Farhat took $15,000 in cash to help draft the REAs the company submitted to the Defense Department, and another $22,000 in cash to recommend that the Navy certify completion of the construction projects and approve the REAs. Following those meetings, Farhat urged the Defense Department to approve the majority of the REAs, without disclosing that defendant had received cash from the company in exchange for his recommendation. (Source)

DoD Employee Sentenced To Prison For The Unauthorized Sale Of Materials From USN Base / Received $300,000+ In Kickbacks - August 25, 2020

Jeffery Parsons was sentenced to one year in prison for conspiring to accept illegal gratuities on account of official actions and conspiring to sell government property without authority.

According to court documents, Parsons was a civilian employee of the U.S. Department of Defense. In November 2009, Parsons began working as an Environmental Protection Specialist at Sierra Army Depot in Herlong, California (SIAD). He later held the same position at Naval Air Station Lemoore in Lemoore, California (NASL). In his official positions at SIAD and NASL, Parsons' responsibilities included the disposition of hazardous materials such as batteries, fuel and oil.

In October 2012, Parsons, his wife, and their associate Travis Wong agreed that Parsons would use his authority at SIAD to allow Wong to sell valuable materials from the installation and that, in return, Wong would pay Parsons and his wife a portion of his proceeds from the sales. After Parsons transferred to NASL, Parsons, his wife, and Wong continued their illegal scheme. Just as Parsons had done at SIAD, he abused his authority at NASL by allowing Wong to sell materials removed from the U.S. Navy base. Once again, Wong paid Parsons and his wife a portion of his proceeds from the sales. In total, Wong received approximately $314,000 from selling government property, and he paid Parsons and his wife approximately $56,000. Wong made the illegal payments by checks payable to a company registered to Parsons' wife, as well as checks payable to Parsons' daughter. (Source)

USN Warehouse Manager Sentenced To Prison For Stealing / Selling $2.5 Million Worth Of Goods From Navy - August 24, 2020

Herbert Gutierrez, former warehouse manager at the U.S. Navy Military Sealift Command (MSC) Warehouse in San Diego and 20-year veteran of the U.S. Navy, was sentenced in federal court today to 24 months in custody for stealing more than $2.5 million worth of goods from the Navy warehouse where he worked.

Gutierrez began stealing from the warehouse for his own personal gain a few months after he started working there. For approximately nine months, between July 2018 and April 2019, Gutierrez advertised items from the warehouse for sale online, including through such websites as eBay, and then allowed private individuals into the MSC warehouse yard during work hours and after hours to take the government property, load it onto trucks, and haul it away. (Source)

LARGEST U.S. NAVY BRIBERY SCHEME IN MILITRAY HISTORY

DoD Contractor Bribed USN Officers For 20+ Years

Leonard Glenn Francis, better known as "Fat Leonard," is a 6 feet, 3 inch tall, 350 pound former Malaysian defense contractor who bribed hundreds of U.S. Navy officers for classified information for more than 20 years. He eventually defrauded the U.S. government and American taxpayers out of at least $35 million dollars until he was caught in a sting operation in 2013. After Francis' arrest, nearly 1,000 Navy officers came under scrutiny, including 91 admirals.

This is one of the biggest bribery investigations in U.S. military history. So far the investigation has resulted in the conviction and sentencing of nearly two dozen U.S Navy officials, defense contractors and others on various fraud and corruption charges. .

The Washington Post reported that in 2007, the Navy's Inspector General forwarded a document claiming GDMA was grossly overcharging the Navy for providing port security but the Naval Criminal Investigative Service (NCIS) may have failed to follow up on the warning. So this is why the bribery scheme continued.

U.S. federal prosecutors filed criminal charges against 33 individuals in connection with the Fat Leonard scandal. Of those, 22 pleaded guilty: Francis himself,4 of his top aides, and 17 Navy officials, specifically, at least 10 commissioned officers, 2 petty officers, 1 former NCIS special agent, and 2 civilian Navy contracting officials. 9 others are awaiting trial in U.S. District Court in San Diego. Separately, 5 Navy officers were charged with crimes under the Uniform Code of Military Justice (UCMJ) and were subject to court-martial proceedings.

According to investigators, by November 2017, more than 440 people, including 60 admirals have come under scrutiny under the inquiry (Source)

DoD Contractor Owner Sentenced To Prison For Massive USN Bribery & Contracting Fraud Scheme - November 5, 2024

Leonard Glenn Francis, mastermind of an unprecedented bribery and fraud scheme targeting the U.S. Navy, was sentenced in federal court To 180 months in prison and ordered to pay $20 million in restitution to the Navy and a $150,000 fine. Francis was also ordered to forfeit $35 million in ill-gotten proceeds from his crimes.

According to admissions in his initial 2015 plea agreement, and other court documents, Leonard Francis and his company, Glenn Defense Marine Asia, or GDMA, provided services to U.S. Navy ships in Asia Pacific ports.

Francis also admitted to defrauding the U.S. Navy of tens of millions of dollars by routinely overbilling for goods and services provided, including fuel, tugboats, and sewage disposal.

Francis gave co-conspirators millions of dollars in things of value, including over $500,000 in cash; hundreds of thousands of dollars in the services of prostitutes and associated expenses; hundreds of thousands of dollars in travel expenses, including airfare, often first or business class, luxurious hotel stays, incidentals, and spa treatments; hundreds of thousands of dollars in lavish meals, top-shelf alcohol and wine, and entertainment; and hundreds of thousands of dollars in luxury gifts, including designer handbags and leather goods, watches, fountain pens, Kobe beef, Spanish suckling pigs, designer furniture, Cuban cigars, consumer electronics, ornamental swords, and hand-made ship models.

Francis admitted that in return, U.S. Navy personnel and command staff advocated on behalf of Francis and his company during the procurement process and provided classified information about various U.S. Navy ships' port visits, proprietary U.S. Navy information such as details about competitors' bids for U.S. Navy contracts, and information about Naval Criminal Investigative Service and U.S. Navy investigations into GDMA's practices, among other things.

In his 2015 plea agreement, Francis also admitted to defrauding the U.S. Navy of tens of millions of dollars by routinely overbilling for goods and services provided, including fuel, tugboats, and sewage disposal.

Over the course of several years, Francis met with government investigators dozens of times to discuss unprecedented levels of corruption within the U.S. Navy. Francis provided detailed information about hundreds of Sailors, from petty officers to admirals, and turned over financial records, photographs, receipts and Navy contracting documents. Corroborated information from Francis substantially assisted the United States in its investigation. (Source)

USN Assistant Chief Of Staff (Seventh Fleet) Sentenced To Prison In Massive Corruption Scandal - February 23, 2023

U.S. Navy Captain (Retired) Jesus Vasquez Cantu was sentenced today to 30 months in prison on charges that he received lavish bribes from foreign defense contractor Leonard Francis

Cantu acknowledged that Francis took him and others out for drinks and dinners at posh restaurants, nightclubs and karaoke bars and paid for lavish hotel rooms and the services of prostitutes on numerous occasions in 2012 and 2013, during which time Cantu was the Deputy Commander in the Far East in Singapore.

Cantu was in charge of logistical sustainment to Navy ships operating in the Seventh Fleet. Cantu admitted that in return for these luxuries, he provided proprietary U.S. Navy information to Francis, and that he used his power and influence to help Francis and his company, Glenn Defense Marine Asia, known as GDMA, in its ship husbanding business. (Source)

4 USN Officers Convicted Of Accepting Bribes From Defense Contractor - June 29, 2022

Former U.S. Navy Captains David Newland, James Dolan and David Lausman and former Commander Mario Herrera, all of whom once served in the Navy's Seventh Fleet, were convicted for accepting bribes from foreign defense contractor Leonard Francis.

9 members of the U.S. Navy's Seventh Fleet, including the 4 defendants convicted today, were indicted by a federal grand jury in March 2017.

This long-running fraud and bribery investigation has resulted in federal criminal charges against 34 U.S. Navy officials, defense contractors and the GDMA corporation. 29 previously pleaded guilty. With today's four convictions, 33 defendants have now been convicted of various fraud and corruption offenses. (Source)

USN Commander Pleads Guilty In Navy Bribery Scandal Involving Fancy Dinners, Hotels, Parties & Prostitutes From Foreign Defense Contractor - February 2, 2022

Former U.S. Navy Captain Donald Hornbeck pleaded guilty to bribery charges, admitting that while he directed the operations of all combatant ships in the Seventh Fleet, he accepted at least $67,830 in extravagant dinners, hotels, parties and prostitutes from foreign defense contractor Leonard Francis in exchange for breaching his official duty to the U.S. Navy.

Hornbeck admitted that he corruptly used his official position to benefit Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia (GDMA). GDMA serviced U.S. Navy ships in the Asia Pacific region. Hornbeck admitted that he endeavored to send Navy ships into ports serviced by GDMA; shared confidential Navy information with Francis in order to help GDMA; and helped with evaluating and indoctrinating potential new Navy members to help Francis.

Hornbeck was one of nine members of the U.S. Navy's Seventh Fleet indicted by a federal grand jury in March 2017 for conspiring with Francis and for receiving bribes. (Source)

USN Commander Pleads Guilty In Navy Bribery Scandal Involving Meals, Entertainment, Travel, Hotel Expenses, Gifts, Cash, & Prostitutes - January 26, 2022

U.S. Navy Commander Stephen Shedd pleaded guilty to bribery charges, admitting that he and 8 other leaders of the U.S. Navy's Seventh Fleet received more than $250,000 in meals, entertainment, travel and hotel expenses, gifts, cash and the services of prostitutes from foreign defense contractor Leonard Glenn Francis.

The remaining defendants are accused of conspiring to trade military secrets and substantial influence for sex parties with prostitutes and luxurious dinners and travel, among other lavish things of value, to include U.S. Navy Rear Admiral Bruce Loveless; Captains David Newland, James Dolan, David Lausman and Donald Hornbeck; and Commander Mario Herrera.

The overarching fraud and bribery investigation has resulted in federal criminal charges against 34 U.S. Navy officials, defense contractors and the GDMA corporation. So far, 28 of those have pleaded guilty, admitting collectively that they accepted millions of dollars in luxury travel and accommodations, meals, lavish gifts, or services of prostitutes, among other things of value, from Francis in exchange for helping GDMA win and maintain contracts and overbill the Navy by over $35 million. (Source)

USN Chief Warrant Officer Pleads Guilty To Receiving $45,000+ In Bribes From Foreign Defense Contractor - August 31, 2021

Chief Warrant Officer Robert Gorsuch admitted in court he received more than $45,000 in bribes from foreign defense contractor Leonard Francis, who provided him with stays at luxurious hotels plus meals, entertainment and other gifts in exchange for official acts that would help Francis' ship husbanding business, including the disclosure of multiple classified ship schedules.

Gorsuch was one of 9 members of the U.S. Navy's Seventh Fleet indicted in March 2017 for participating in a conspiracy with Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia. (Source)

U.S. Marine Corps Colonel Pleads Guilty To Accepting $67,000+ In Bribers From Foreign Defense Contractor - September 3, 2021

U.S. Marine Corps Colonel Enrico DeGuzman pleaded guilty to a bribery charge, admitting that he accepted more than $67,000 in extravagant meals, drinks, entertainment and hotel stays in Hong Kong, Singapore, and Tokyo from foreign defense contractor Leonard Glenn Francis.

DeGuzman admitted that in return for this and other things of value, he corruptly used his official position to assist Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia, a ship husbanding company that serviced U.S. Navy ships in the Asia Pacific region. DeGuzman admitted that he endeavored to influence Navy ships into ports serviced by GDMA; he shared confidential Navy information with Francis in order to help GDMA; and he helped with evaluating and indoctrinating potential new Navy members into Francis's cabal.

In one instance, DeGuzman joined Francis and others for a $40,000 meal that featured foie gras terrine, duck leg confit, ox-tail soup, and roasted Chilean sea bass, paired with expensive wine and champagne, followed by digestifs, cigars and overnights at the Shangri La - all at Francis's expense.

DeGuzman was one of nine members of the U.S. Navy's Seventh Fleet indicted by a federal grand jury in March 2017 for conspiring with Francis and for receiving bribes. DeGuzman is the second of the Seventh Fleet defendants to plead guilty. The trial of the remaining defendants was scheduled to begin November 1, 2021, but yesterday it was postponed until February 7, 2022. The remaining defendants - who are accused of trading military secrets and substantial influence for sex parties with prostitutes and luxurious dinners and travel - include U.S. Navy Rear Admiral Bruce Loveless; Captains David Newland, James Dolan, Donald Hornbeck and David Lausman; Commander Stephen Shedd; and Commander Mario Herrera.

The overarching fraud and bribery case has resulted in federal criminal charges against 34 U.S. Navy officials, defense contractors and the GDMA corporation. So far, 27 of those have pleaded guilty, admitting collectively that they accepted millions of dollars in luxury travel and accommodations, meals, or services of prostitutes, among many other things of value, from Francis in exchange for helping GDMA win and maintain contracts and overbill the Navy by over $35 million. (Source)

USN Chief Petty Officer Sentenced To Prison For Bribery Conspiracy With Foreign Defense Contractor - October 30, 2020

Brooks Parks, a U.S. Navy Chief Petty Officer, is that latest to be sentenced in the wide-ranging corruption and fraud investigation involving foreign defense contractor Leonard Francis and his Singapore-based company, Glenn Defense Marine Asia (GDMA).

Francis pleaded guilty in 2015 to bribery and fraud charges, admitting that he presided over a massive, decade-long conspiracy involving scores of U.S. Navy officials, tens of millions of dollars in fraud and millions of dollars in bribes - from cash, prostitutes and luxury travel accommodations to Cuban cigars, Kobe beef and Spanish suckling pigs.

So far, 34 defendants have been charged and 23 have pleaded guilty as part of this investigation, many admitting they accepted luxury travel and accommodations, meals or services of prostitutes from Francis in exchange for helping GDMA win and maintain contracts and overbill the Navy by millions of dollars.

From December 2005 to February 2009 Parks served as the Logistics Lead Petty Officer on the USS Blue Ridge, the command ship for the Seventh Fleet. Parks was actively involved in managing the Seventh Fleet's logistics support budget, signing and processing invoices, and performing other supervisory logistics functions for the Seventh Fleet.

Parks admitted that from March 2006 through March 2010, Francis paid for lavish hotel accommodations for Parks and his friends throughout Asia, as the USS Blue Ridge came into port. Parks had expensive taste and wasn't restrained in demanding ever more luxuriant accommodations from GDMA. In one instance, Parks demanded the $4,800 per night Ritz Carlton Suite in Singapore, though he was ultimately provided

In return for these bribes, Parks approved and expedited GDMA invoices and payment requests, provided substantial bidding and pricing information to GDMA as part of GDMA's effort to crush its competitor in the Philippines, and provided limited ship port visit scheduling information. (Source)

U.S. MARINES (USM)

Office Manager Sentenced To Prison For $1.3 Million Fake Invoice Fraud Scheme For USM Forces Reserve - July 31, 2024

Kamila Dudley employed by Company A from September 2008 through March 2023; and, from March 2017 through November 2018. Dudley erved as Company A's Office Manager. As Company A's Ofice Manager, Dudeley prepared and submitted Company A's invoices for payment.

In approximately March 2017, Company A subcontracted with Company B to provide onsite support services at the Marine Forces Reserve (MARFORRES) facility in New Orleans, Louisiana. Company A, by and through multiple employees, committed wire fraud by knowingly submitting materially false invoices to Company B, knowing that Company B would, in turn, present the false information to the United States for payment. From March 2017 through November 2018, Company A billed the United States, through Company B, for services not provided.

The fraudulent invoices included the names of Company A's executives, who performed no work at MARFORRES. The fraudulent invoices also included the names of certain individuals who worked full-time on a separate contract at a separate facility and, thus, performed no work at MARFORRES. Because neither Company B nor the United States was aware of the fraudulent nature of the invoices, Company A was paid approximately $1,300,000 under the subcontract. (Source)

USM And USN Sailor Sentenced To Prison For $65 Million+ Tricare / Military Healthcare Program Fraud Scheme - April 12, 2024

Former U.S. Marine Joshua Morgan and former U.S. Navy Sailor Kyle Adams were sentenced to 21 months and 15 months, respectively, and ordered to pay millions in restitution and forfeit the fruits of their criminal activity.

Morgan and Adams have admitted that they recruited fellow servicemembers and their dependents to receive expensive prescription compounded drugs, while others in the conspiracy wrote bogus prescriptions and filled out duplicitous paperwork to process fraudulent insurance reimbursements, resulting in at least $65 million in losses to TRICARE.

According to plea agreements, the servicemembers that Morgan and Adams recruited agreed to receive the pricey compounded medications in return for a monthly kickback of approximately $300. For young Sailors and Marines this money was equivalent to a significant portion of their monthly paycheck. Morgan noted that "it took very little work to sign people up to receive free money."

For recruiting bogus patients, defendants Morgan and Adams were paid an illegal kickback of between 3 and 7 percent of the total TRICARE reimbursement paid to the pharmacy for the drugs sent to their recruits. By the time this fraud scheme was in full swing, the average cost for these compounded drugs was over $13,000 for a 30-day supply, peaking at around $25,000 for individual drugs.

Over the course of the conspiracy, those illegal kickbacks amounted to at least $2,633,942.69 for Morgan, which, in recognition of his role as the top-level recruiter in this multi-level marketing scheme, was more than twice as much as the next nearest patient recruiter. Meanwhile, Adams earned more than $1 million for his efforts. (Source)

USM Pleads Guilty To Gun Trafficking Charges - March 1, 2024

Rylan Peterson while serving as a private first class in the Marine Corps at a base in North Carolina, admitted that he entered into an agreement with Oryn McLeod, for Peterson to acquire six semi-automatic handguns on behalf of McLeod and others.

Peterson then obtained the guns from North Carolina resident Mitchell Locke, who purchased them from a licensed dealer in North Carolina, falsely representing at the time of the purchase that he was acquiring the firearms for himself. McLeod paid Peterson for the guns, which Peterson transported to New York from North Carolina. McLeod was subsequently arrested for unlawful possession of two of the handguns. (Source)

USM Reservist Sentenced To Prison For Stealing, Forging, Selling & Distributing Fraudulent COVID-19 Vaccination Cards - April 6, 2024

Jia Liu was sentenced to 21 months in prison for conspiring to steal, forge and distribute fraudulent COVID-19 Vaccination Cards.

On June 9, 2023, co-defendant Steven Rodriguez, a Long Island nurse, was sentenced to 30 months' imprisonment for his role in the same scheme. Liu and Rodriguez pleaded guilty in April 2023 to conspiracies to defraud and obstruct the United States' response to the COVID-19 pandemic.

In May 2021, Liu and Rodriguez conspired to steal, forge, sell and distribute COVID-19 Vaccination Cards to hundreds of unvaccinated persons. In addition to the cards, Liu and Rodriguez also offered buyers and co-conspirators false entry into government immunization databases.

Liu specifically targeted the armed forces and their attempts to contain the COVID-19 pandemic. From approximately August 2021 or earlier, the defendant created and distributed false COVID-19 Vaccination Cards to members of the U.S. Marine Corps Reserve to help them evade its vaccination requirements. Liu boasted to a co-conspirator on an encrypted messaging app: "you have no idea how many documents I have faked in my usmc (United States Marine Corps) career." (Source)

USM Arrested On Charges Stemming From Role In Firebombing Of Planned Parenthood Clinic - June 14,2023

Agents with the FBI and the Naval Criminal Investigative Service arrested two men on federal charges alleging they used a Molotov cocktail to firebomb a California Costa Mesa clinic operated by Planned Parenthood Federation of America.

Chance Brannonstrano was an active duty Marine stationed at Camp Pendleton, and the other individual involved was Tibet Ergul.

Ergul and Brannon attacked the clinic during the early morning hours of March 13, 2022, by igniting and a throwing a Molotov cocktail at the clinic entrance. As a result of the fire, the Planned Parenthood Costa Mesa healthcare clinic was forced to close the following morning and cancel approximately 30 appointments.

Security videos described in the affidavit show that two men wearing hooded sweatshirts and face masks approached the Planned Parenthood facility at approximately 1 a.m. the day of the attack, ignited a device, and threw the flaming device at the front door of the building. The device landed against a southern wall next to the glass door and erupted into a fire, which spread up the wall and across the ceiling above the glass door. (Source)

USM Official Sentenced To Prison For Taking $100,000 In Bribes For Directing $2 Million+ Worth Of Transportation Contracts To Bus Company - July 1, 2021

In 2019 Darrel Fitzpatrick was a senior account manager at a bus brokerage company that provided transportation to the United States Marine Corps (USMC) Reserves. That same year, Fitzpatrick started a competing transportation brokerage company called National Charter Express.

In 2019, Fitzpatrick agreed to pay kickbacks to Erik Martin, a civilian employee of the USMC Reserves, in exchange for Martin directing business to the bus company, and then later, National Charter Express. The conspiracy resulted in at least $2,000,000 in transportation contracts being corruptly awarded to companies associated with Fitzpatrick over six months in 2019. In exchange, Fitzpatrick wired and attempted to wire Martin over $250,000 in bribes in a series of at least four transactions. (Source)

USM Sentenced To Prison For Illegal Exportation Of Firearms And Controlled Equipment To Haiti - March 2, 2021

On December 12, 2020, Jacques Duroseau was convicted of conspiracy to illegally export and smuggle firearms and controlled equipment from the United States to Haiti, as well as transporting firearms without a license to the Haitian Army.

At trial, the evidence showed that Duroseau, at the time an active duty U.S. Marine with the rank of sergeant, along with a co-conspirator, both impersonated high ranking military officers and pretended to be on military business in order to facilitate the illegal transportation of eight firearms, including a Ruger model Precision Rifle 300WIN MAG and a Spike's Tactical model ST15, as well as copious ammunition, riflescopes, and body armor, via commercial aircraft to Haiti. The evidence further showed that Duroseau's purpose was to train the Haitian Army with the firearms and equipment in order to engage in foreign armed conflict. (Source)

NATIONAL GUARD

National Guardsman Convicted For Providing Illegal Alien Smuggling Group Assistance & Law Enforcement Information - August 29, 2024

Derrick Terelle Sankey, a native of Alabama, was serving under the authority of the Department of Homeland Security (DHS) in the Rio Grande Valley, Texas in 2021.

From March to September 2021, conspirators recruited Sankey into an existing alien smuggling group in which he would provide insight into counter-smuggling activities. He also scouted for vehicles he knew contained individuals who were illegally present in the United States in order to thwart law enforcement from detecting them.

Sankey also admitted to providing law enforcement information to an alien smuggling organization. He also worked as a scout when loads of aliens would move from Starr and Hidalgo Counties to near the Border Patrol Checkpoint in Jim Wells County. (Source)

U.S. DEPARTMENT OF VETERANS AFFIRS (VA)

VA Medical Center Employee Charged With $20,000 COVID Paycheck Protection Program Fraud - November 7, 2024

Lakeysha Day was an employee of the U.S. Department of Veterans Affairs. She worked at the V.A. Medical Center in Columbia, Mo., at the time of the offense.

According to today's indictment, Day applied for a Paycheck Protection Program (PPP) loan for her business on March 20, 2021. The CARES Act established several new temporary programs and provided for the expansion of others to address the COVID-19 pandemic. The PPP authorized forgivable loans to small businesses to retain workers and maintain payroll, make mortgage interest payments, lease payments, and utility payments.

Day claimed to be a sole proprietor of a business which had an average monthly payroll of $8,000. The supporting documents she submitted claimed gross receipts or sales of $114,210, business expenses of $14,685 and a profit of $99,525. In reality, however, Day's 2019 personal income tax return did not report income and expenses that were claimed in the loan application. (Source)

Day fraudulently obtained $20,000 under the PPP. (Source)

3 VA Employees Charged With $80,000+ Of COVID-19 Pandemic Relief Fraud - August 21, 2024
Katherine Liggins is facing one count of wire fraud and one count of material false statement for allegedly lying to acquire more than $20,000 in PPP funds.

Eric Scott is facing one count of wire fraud and one count of material false statement for allegedly applying for and spending more than $20,000 in PPP funds under false pretenses.

Tamika Wilson is facing two counts of wire fraud, two counts of material false statement and two counts of material false document. Wilson is accused of applying for and receiving more than $40,000 in PPP loans she was not entitled to. (Source)

12 Veterans Affairs Employee Under Investigation For Unauthorized Access To The Medical Records Of Both Vice Presidential Nominees - September 30, 2024
At least a dozen staffers at the U.S. Department of Veterans Affairs improperly accessed the medical records of both vice presidential nominees, Republican Sen. JD Vance, of Ohio, and Democratic Minnesota Gov. Tim Walz, over the summer.

Those employees are under criminal investigation for potentially violating federal health privacy laws. The unauthorized views were uncovered by Veterans Affairs investigators, who notified the Vance and Walz campaigns.

Law enforcement officials stated that the VA Inspector General Michael Missal's office shared evidence with federal prosecutors related to several health system employees, including a physician and a contractor who "spent extended time" viewing the medical files of former President Donald Trump and Vice President Kamala Harris' running mates.

The VA employees under investigation, including the physician and contractor, accessed the medical records using their VA computers and did so mostly from their government offices. Some of the staffers in question reportedly told investigators they were simply curious to see the files of Vance and Walz given both candidates have defended their military records on the campaign trail. (Source)

VA Psychologist Sentenced To Prison For $35,000+ Medicare Fraud Scheme - May 1, 2024
Theresa Kelly was employed in southern Illinois as a Psychologist with the Department of Veterans Affairs.

Kelly engaged in a scheme to defraud Medicare and obtain payment for psychiatric services that she did not provide to residents of a Southern Illinois nursing home between May 2016 and January 2018. In addition to her full-time job at the VA, Kelly owned a company by the name of TS Onsite Mental Health through which she claimed to provide psychotherapy sessions to patients at Shawnee Christian Nursing Center in Herrin, Illinois. Kelly billed Medicare for more than 400 claims, worth more than $54,000, for services that she did not provide. Kelly billed for at least some of the services on days she was on approved medical leave from the VA. Kelly was ordered to repay $35,795.94 in restitution to the Centers for Medicare & Medicaid Services as repayment for her fraudulent claims. (Source)

VA Procurement Supervisor Sentenced To Prison For Receiving $36,000+ In Kickbacks For 7 Years - April 15, 2024

While serving as a Procurement Supervisor at Veterans Affairs Medical Center in Chicago, Thomas Duncan received thousands of dollars in kickbacks paid in cash and checks from Daniel Dingle, the President of a medical supply company in Dolton, Illinois.

Duncan received approximately $36,250 in kickbacks paid by checks, as well as an additional amount in cash, from Daniel Dingle, the president of a medical supply company.

The checks were made payable to Helping Hands Properties LLC, a third-party entity managed by Duncan, that contained false and misleading memo entries in order to conceal and disguise the existence and purpose of the kickbacks. In exchange for the kickbacks, Duncan used his official position at the VA to fraudulently initiate and approve purchases of products from Dingle's company, knowing that many of the products would not actually be delivered to the VA.

The fraud scheme began in 2012 and continued until 2019. In late 2018, after Duncan became aware that the VA Inspector General's Office was investigating his conduct, Duncan created fake invoices from Helping Hands purporting to document work performed for Dingle's company. Duncan also told Dingle to falsely tell investigators that the payments Duncan received from Dingle's company were for work performed by Helping Hands.

Duncan was ordered to pay $1,709,344 in restitution. (Source)

VA Medical Center Pharmacy Employee Sentenced To Prison For Role In Stealing / Selling Diabetic Test Strips Worth $427,000+ - February 7, 2024

Jennifer Robertson was employed at the Battle Creek Veterans Affairs (VA) Medical Center Pharmacy in Michigan. She was responsible for ordering supplies for veterans in need of medical care.

Beginning in June 2017, Robertson stole diabetic test strips from pharmacy inventory and arranged to meet Michelle McAllister and sell them for cash. McAllister in turn sold and shipped them to Steven Anderson in Pennsylvania. Their scheme unraveled when Robertson was caught stealing in November 2019.

In June 2023, a jury found Anderson guilty of all twelve charges against him. In total, Anderson trafficked over 7,900 boxes of stolen diabetic test strips worth over $427,795. Anderson's co-conspirators, Robertson and McAllister pled guilty and were sentenced to prison last year. (Source)

VA Nurse Sentenced To Prison For Role In Leading $3.5 Million Unemployment Insurance Fraud Scheme - August 23, 2023

From April 2020 through March 2021, Heather Huffman lead and organized several others, including family members and close friends, in a conspiracy to defraud at least five state workforce agencies, including the Virginia Employment Commission, the Washington State Employment Security Department, and the California Employment Development Department, of more than $3.5 Million in unemployment insurance benefits.

Huffman's conspiracy specifically targeted benefits that had been expanded to offset the economic impacts of the COVID-19 pandemic. Huffman and others filed false and misleading applications in the names of identity theft victims, witting co-conspirators, and inmates of state and federal prisons.

Huffman and her conspirators included in these applications materially false wage and employment histories and false contact information, such as physical and mailing addresses, email addresses, and phone numbers, that did not, in fact, belong to the purported applicants.

Huffman and her conspirators submitted more than 220 applications in the names of more than 120 individuals to at least five different states through which they sought to receive more than $3.5 Million and actually obtained more than $2 Million.

Huffman's sentencing was originally scheduled for November 29, 2022, but she failed to appear that day without notice or explanation. Prior to her disappearance, Huffman took measures to flee prosecution and conceal her whereabouts, including depleting her bank accounts, selling her vehicle, and turning her phone off. Through means unknown, Huffman obtained the PII of a real person, assumed that person's identity, and procured counterfeit government identification and credit cards in the name of her false alias. Following Huffman's disappearance, the United States Marshals Service (USMS) opened a fugitive investigation. This extensive, months-long investigation uncovered evidence that the defendant, under a false identity, was living and working as a registered nurse in Kansas. On March 4, 2023, approximately 95 days after Huffman's flight from prosecution, she was apprehended by the USMS in Kansas at an Extended Stay hotel. (Source)

VA Hospital Employee Sentenced To Prison For Stealing Almost $487,000 In Government Funds - September 22, 2022

Bruce Minor pleaded guilty to one count of theft of government funds. The charge arose from his theft of approximately $487,000 in Veterans Affairs travel reimbursement funds, which he helped administer as part of his official duties as a travel clerk.

In order to perpetrate the theft, Minor created fraudulent travel reimbursement claims in the names of at least three other VAMC employees and then diverted the fraudulently obtained funds into bank accounts he controlled. (Source)

VA Hospital Nurse Pleads Guilty To Stealing COVID19 Vaccination Cards & Selling Them On Facebook - June 17, 2022

Bethann Kierczak was a registered nurse with the Veteran's Hospital in Detroit.

Kierczak admitted to stealing or embezzling authentic Covid-19 Vaccination Record Cards from the VA hospital, along with vaccine lot numbers necessary to make the cards appear legitimate. She then resold those cards and information to individuals within the metro Detroit community. Kierczak's theft of Covid-19 Vaccination Record Cards began at least as early as May 2021 and continued through September 2021. Kierczak sold the cards for $150-$200 each and communicated with buyers primarily via Facebook Messenger. (Source)

VA Medical Center Procurement Officer Sentenced To Prison For Stealing $8.2 Million+ Worth Of HIV Medication And Selling - May 26, 2022

From October 2015 through November 2019, Lisa Hoffman was a procurement officer for the pharmacy of the Veterans Affairs Medical Center (VAMC) in East Orange, New Jersey.

Hoffman used her authority to order medication for the outpatient pharmacy, including ordering large quantities of HIV medication. Hoffman admitted that she stole HIV prescription medications from the VAMC pharmacy and sold it to her conspirator Wagner Checonolasco, in exchange for cash.

Checonolasco previously admitted to conspiring with Hoffman to steal HIV medication belonging to the U.S. Department of Veterans Affairs. The loss amount was more than $8.2 million. (Source)

VA Employee Sentenced To Prison For Stealing Personal Protective Equipment & Other Medical Equipment, Then Selling And Making $50,000+ - January 7, 2022

Chad Jacob stole personal protective equipment (PPE), electronics, and medical equipment while working as the Assistant Chief of Supply Chain Management for the Gulf Coast Veterans Health Care System.

Starting in 2019 and continuing to December 2020, Jacob stole items belonging to the VA and resold them to local pawn stores and on his personal eBay account. In total, Jacob made more than $50,000 selling the stolen N-95 masks and over $9,000 selling stolen iPads and iPhones. (Source)

VA Employee Sentenced To Prison Defrauding The VA Of $183,000+ Over 5 Years Claiming He Was Disabled - December 6, 2021

Anthony Medrano admitted that between approximately November 2015 and May 2020, he submitted claims to the Veterans Administration (VA) in which he purported to be disabled so that he could obtain caregiver benefits for his wife, when he was actually able-bodied and even participating in fitness challenges and coaching youth sports.

Medrano executed this scheme while employed in the VA's Veterans Benefits Administration as a Veterans Service Representative. Using the knowledge gained from his VA employment, Medrano stole $183,034.38 from the VA through a series of lies. (Source)

VA Purchasing Agent Sentenced To Prison For Theft Of $1.9 Million Of VA Equipment - Which He Then Sold - December 1, 2021

Kevin Rumph was employed by the Veterans Administration (VA) as a purchasing agent since 2012.

Rumph used his VA issued credit card to buy over $1.9 million worth of Continuous Positive Airway Pressure (CPAP) equipment. He then stole and sold the CPAP supplies to a vendor located in Ohio. CPAP supplies are medical products used to treat obstructive sleep apnea. Between 2013 to 2021, Rumph made hundreds of unauthorized CPAP supply purchases costing the VA in excess of $1.9 million. (Source)

2 VA Employees Charged With Pocketing Over $250,000 In Cash From Vendors For Kickbacks - November 17, 2021

2 employees of the U.S. Department of Veterans Affairs pocketed cash from vendors in exchange for steering them orders for medical equipment, according to indictments returned in federal court in Chicago.

Andrew Lee and Kimberky Dyson worked as Prosthetic Clerks in the Veterans Health Administration Prosthetics Service in Chicago. As part of their duties, Lee and Dyson selected vendors from which to order medical equipment for VA patients, and then paid the vendors using government purchase cards. In exchange for their efforts with certain vendors, Lee and Dyson allegedly received cash payments from individuals at the vendor companies, in exchange for steering them orders for medical equipment. Lee pocketed kickbacks of at least $220,000. Dyson accepted at least $39,850. (Source)

VA Supervisor Sentenced To Prison For Receiving Kickbacks & The Theft Of $1 Million+ Of Government Property - October 14, 2021

From October of 2010, through January of 2019, William Precht worked as an Inventory Management Specialist and later as a Supervisory Management and Program Analyst at the Cleveland VA Medical Center. Through his positions at the VA, Precht could order medical supplies, purchase capital equipment and monitor requests for equipment purchases.

Using his position and his VA employee log-in information, Precht registered a purported vendor (Vendor-1) as a Small Disadvantaged Business and Veteran-Owned Small Business in the VA vendor system. Beginning in October of 2010, Precht used his VA purchase card and other employee cards to purchase purported medical supplies from Vendor-1, a company he controlled, in the amount of approximately $1,066,348.

In addition, from May of 2015 through January of 2019, Precht conspired with Robert A. Vitale, a medical sales representative for multiple companies that conducted business with the Cleveland VA, to devise a scheme in which Precht would receive kickbacks and other items of value, in exchange for steering VA business and other monetary awards to Vitale.

In order to conceal his schemes, Precht provided false and misleading information to VA employees about reasons for ordering medical supplies and falsified patient records. As a result, the Cleveland VA suffered a loss of $193,042.66.

Robert. A. Vitale pleaded guilty on October 13, 2021 for his role in the scheme. (Source)

VA Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences for Murdering 7 Veterans - May 11, 2021

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (V in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

VA Employee Sentenced To Prison For A Stealing & Attempting To Sell Veterans' Personal Information - May 25, 2021

In the fall of 2017, federal agents learned that Phillip Hill, who worked at the North Little Rock Veterans Affairs (VA) Medical Center as a Program Analyst, had access to veterans' and current VA employees' personal information to include names, dates of birth, and social security numbers.

Hill had contacted another individual and attempted to sell personal identifying information to a buyer for approximately $100,000. Multiple recorded conversations with this individual and Hill were monitored by agents. Throughout one monitored conversation, Hill repeatedly acknowledged the illegality of his conduct. Hill explained that he was offering to sell the personal identifying information for any veteran who had received VA compensation or a pension, visited a VA medical center, or had completed a VA financial assessment. Hill also offered to sell personal identifying information for VA employees, explaining the employees data would be particularly valuable to identity thieves, as it would include personal identifying information and personal account information for employees who were earning over $50,000 a year. (Source)

VA Employee Sentenced To Prison For Accepting $21,500+ In Bribes For $1 Million In Grants - May 12, 2021

Daniel Ross worked for the U.S. Department of Veterans Affairs (VA) in Fayetteville, North Carolina, as an agent for the Specially Adapted Housing (SAH) grant program, which provides federal funds to eligible veterans with certain severe, service-connected disabilities for the purpose of constructing adapted homes or modifying existing homes.

During the offense period, Ross was the assigned SAH agent for multiple grant projects awarded to All American Home Renovations (AAHR), a Fayetteville-based construction company then-owned and operated by Marc Schantz. Ross abused his position as an SAH agent to steer over $1 million worth of grant projects to AAHR in exchange for monetary payments from Schantz. Ross routinely advised his VA supervisors to approve grant awards to veterans in which AAHR was improperly and deceptively designated as a particular veteran's "builder of choice" when, in fact, Ross had misled the veteran to believe that AAHR had been selected for them by the VA. AAHR concealed the unlawful payments to Ross by transferring the funds to a dormant business owned by Ross, making it appear as if the business was providing legitimate subcontracting services to AAHR.

Ross previously pled guilty to the charge. He was also ordered to pay $21,520.00 in restitution. (Source)

VA Medical Center Respiratory Therapist Sentenced To Prison For Stealing And Selling $132,000+ Worth Of COVID-19 Respiratory Supplies - January 11, 2021

Gene Wamsley admitted to stealing a ventilator and other respiratory medical equipment in the midst of the COVID-19 pandemic and selling it for his own gain.

The investigation began in January 2020 when VAMC reported two bronchoscopes, used for examining a patient's airway, went missing from the hospital. A third bronchoscope was reported missing in April 2020. In all, Wamsley admits stealing and selling three bronchoscopes worth over $100,000 for just $15,750. Wamsley sold the scopes to a Florida resident via eBay. When Wamsley's home was searched in June, law enforcement seized a fourth bronchoscope and a $6,000 sleep apnea device called a WatchPat that had been stolen from the VA Medical Center. Further investigation revealed that in April 2020, Wamsley also stole a $9,950 respirator and sold it via eBay to an Ohio man for just $6,000.

The total loss to the United States from the thefts is $132,291. (Source)

VA Employee Sentenced To Prison For Receiving $1.5 Million In Kickbacks For $20 Million+ Health Care Fraud Scheme - June 11, 2020

Joseph Prince was one of two Case Management Liaisons for the VA's Spina Bifida (SB) Health Care Benefits Program. The program covers the medial needs of children of certain veterans of the Korea and Vietnam wars with SB.

Prince recruited friends and family members to open "home health agencies" knowing they lacked the necessary medical licenses or credentials to bill the VA for SB beneficiaries' home health services. The defendant directed every aspect of the home health agencies; no changes were made to business operations without his knowledge, review, and approval.

Between June, 2017 and June, 2018, Prince referred approximately 45 SB beneficiaries to the sham home health entities. During that time, the home health entities submitted fraudulent claims totaling over $20 million to the VA, and approximately $18 million of that was paid out to five home health entities from the SB Health Care Benefits Program. Prince benefited from the scheme through payments to one of the companies owned by his wife, and from kickbacks paid to him by two of the agencies. As part of his agreement with these two, Prince received kickbacks of 50% of the VA payments for each beneficiary after expenses. Prince received approximately $1.5 million in kickbacks from two of the home health entities between December, 2017 and June, 2018. (Source)

VA Employee Pleads Guilty To Embezzling $70,000 By Routing Funds To His Personal Bank Account / Avoids Prison Time - May 14, 2020

Michael Donaher worked as an Inventory Management Specialist for the Veterans Affairs Medical Facility in Brockton, Massachusetts, and was responsible for purchasing various equipment necessary for use in the facility.

Donaher conducted fraudulent transactions using his government-issued purchase cards and routed the proceeds to his personal bank account. Donaher attempted to conceal these fraudulent purchases by making it appear as if the purchases were made through a large company that the VA frequently used for legitimate business, when, in fact, they were actually made through a company Donaher created through Square, Inc., a mobile payment company. These purchases were not for actual items ever received by the VA. Furthermore, Donaher attempted to hide this fact by annotating the items as having been received within the VA's accountability system. Donaher fraudulently routed approximately $70,000 of VA funds to his personal account since the scheme began in 2016. (Source)

UPDATE:

Donaher was sentenced to time served, approximately one day, in addition to three years of supervised release, with the first six months to be served in a sober house. Donaher was ordered to pay $69,720 in restitution. (Source)

VA Official Sentenced To Prison For Accepting $4,500+ In Bribes To Rig Federal Contracts - February 26, 2020

Dwane Nevins was a small business specialist at the VA's Network Contracting Office in Colorado.

He agreed to take bribes offered by co-defendants Robert Revis, Anthony Bueno and an undercover FBI agent to help them manipulate the process for bidding on federal contracts with the VA.

Revis and Bueno, working with Nevins, agreed to submit fraudulent bids from service-disabled-veteran-owned small businesses under contract with their consulting company so that federal contracts would be set aside for

only those companies. As Bueno put it, the conspirators would then "own all the dogs on the track." Nevins, Bueno and Revis worked to conceal the nature of the bribe payments by either kicking back to Nevins a portion of the payments made to their consulting company, or by asking their consulting company's clients to pay Nevins for sham training classes related to federal contracting. At one of those sham trainings in Las Vegas, Nevada, Nevins accepted a $4,500 cash bribe from the undercover FBI agent. (Source)

INTELLIGENCE COMMUNITY AGENCIES
CENTRAL INTELLIGENCE AGENCY (CIA)

CIA / White House Employee Arrested For Acting As Agent Of South Korean Government In Return For Personal Enrichment - July 17, 2024

Sue Mi Terry, a former CIA and White House employee, subverted foreign agent registration laws in order to provide South Korean intelligence officers with access, information, and advocacy. Terry allegedly sold out her positions and influence to the South Korean government in return for luxury handbags, expensive meals, and thousands of dollars of funding for her public policy program.

After leaving U.S. government service and for more than a decade, Terry worked as an agent of the government of the Republic of Korea (ROK), commonly known as South Korea, without registering as a foreign agent with the Attorney General, as required by law. As covertly directed by ROK government officials, Terry publicly advocated ROK policy positions, disclosed non-public U.S. government information to ROK intelligence officers, and enabled ROK officials to gain access to U.S. government officials. In return for these actions, ROK intelligence officers provided Terry with luxury goods, expensive dinners, and more than $37,000 in funding for a public policy program focusing on Korean affairs that Terry controlled.

From in or about 2001 to in or about 2011, Terry served in a series of positions in the U.S. government, including as an analyst on East Asian issues for the Central Intelligence Agency, as the Director for Korea, Japan, and Oceanic Affairs for the White House National Security Council, and as the Deputy National Intelligence Officer for East Asia at the National Intelligence Council. Since leaving government service in or about 2011, Terry has worked at academic institutions and think tanks in New York City and Washington, D.C. Terry has made media appearances, published articles, and hosted conferences as a policy expert specializing in, among other things, South Korea, North Korea, and various regional issues impacting Asia. Terry has also testified before Congress on at least three occasions regarding the U.S. government's policy toward Korea. (Source)

CIA Official Charged For Leaking Classified Information About Israel's Plans To Strike Iran - November 13, 2024

Asif Rahman held a Top Secret / Sensitive Compartmented Information (SCI) security clearance as part of his role working for the U.S. government.

On or about Oct. 17, Rahman retained without authorization two documents classified at the Top Secret / SCI level, which contained information relating to national defense, and transmitted those documents to a person not entitled to receive them.

Rahman has been charged with leaking highly classified US intelligence about Israel's potential plan to retaliate against Iran for a missile strike in 2024.

The files, which were prepared by the National Geospatial-Intelligence Agency, in part detailed satellite imagery tied to the potential Israeli strike, as well as the various kinds of missiles on hand. They were posted by a telegram account called "Middle East Spectator." (Source)

CIA Officer Sentenced To Prison For Providing People's Republic Of China Classified Information - September 11, 2024

Alexander Ma of Honolulu, a former Central Intelligence Agency (CIA) officer, was sentenced to conspiring to gather and deliver national defense information to the People's Republic of China (PRC).

Ma was arrested in August 2020, after admitting to an undercover FBI employee that he had facilitated the provision of classified information to intelligence officers employed by the PRC's Shanghai State Security Bureau (SSSB).

Ma worked for the CIA from 1982 until 1989. His blood relative (Co-Conspirator CC #1), who is deceased, also worked for the CIA from 1967 until 1983. As CIA officers, both men held Top Secret security clearances that granted them access to sensitive and classified CIA information, and both signed nondisclosure agreements.

As Ma admitted in the plea agreement, in March 2001, over a decade after he resigned from the CIA, Ma was contacted by SSSB intelligence officers, who asked Ma to arrange a meeting between CC #1 and the SSSB. Ma convinced CC #1 to agree, and both Ma and CC #1 met with SSSB intelligence officers in a Hong Kong hotel room for three days. During the meetings, CC #1 provided the SSSB with a large volume of classified U.S. national defense information in return for $50,000 in cash. Ma and CC #1 also agreed to continue to assist the SSSB.

In March 2003, while living in Hawaii, Ma applied for a job as a contract linguist in the FBI's Honolulu Field Office. The FBI, aware of Ma's ties to PRC intelligence, hired Ma as part of a ruse to monitor and investigate his activities and contacts with the SSSB. Ma worked part time at an offsite location for the FBI from August 2004 until October 2012.

As detailed in the plea agreement, in February 2006, Ma was tasked by the SSSB with asking CC #1 to identify four individuals of interest to the SSSB from photographs. Ma convinced CC #1 to provide the identities of at least two of the individuals, whose identities were and remain classified U.S. national defense information.

Ma confessed that he knowingly and willfully conspired with CC #1 and SSSB intelligence officers to communicate and transmit information that he knew would be used to injure the United States or to advantage the PRC. (Source)

NATIONAL SECURITY AGENCY (NSA)

NSA Contractor Sentenced To Prison For $176,000+ Time & Attendance Fraud - July 3, 2024

Jacky McComber was the Chief Executive Officer of an information technology company that had contracts with the NSA. Because the subject matter of these contracts involved classified information, most of the work had to be performed at a secure location, and there were significant limitations to the amount of work that could be performed off-site.

McComber billed for her supposed work physically at the NSA, when in reality approximately 90% of the work she billed for was not when she physically was at the NSA.

The evidence further showed that McComber at times did not work the number of hours on the contract that she recorded on her timesheets. For example, on occasions when McComber billed a full day to the contract, she participated in charity events, attended a reunion, and was on vacation. As further detailed in trial testimony, McComber participated in a voluntary interview with NSA-OIG investigators as a result of information received from a whistleblower indicating that McComber was billing the government for hours that she was not actually working.

McComber was odered to pay $176,913 in restitution for submitting false invoices to the National Security Agency (NSA) for overstating her hours worked on a contract and for making false statements to investigators from the NSA's Office of the Inspector General. (Source)

NSA Employee Sentenced To Prison For Attempted Espionage - April 29, 2024

Jareh Dalke pleaded guilty in 2023 to six counts of attempting to transmit classified information to a foreign agent.

From June 6 to July 1, 2022, Dalke was an employee of the National Security Agency (NSA) where he served as an Information Systems Security Designer. Dalke admitted that between August and September 2022, in order to demonstrate both his legitimate access and willingness to share, he used an encrypted email account to transmit excerpts of three classified documents to an individual he believed to be a Russian agent. That person was an FBI online covert employee. All three documents from which the excerpts were taken contained classified as Top Secret / Sensitive Compartmented Information (SCI) and were obtained by Dalke during his employment with the NSA.

On or about Aug. 26, 2022, Dalke requested $85,000 in return for all the information in his possession. Dalke claimed the information would be of value to Russia and told the FBI online covert employee that he would share more information in the future, once he returned to the Washington, D.C. area.

Dalke subsequently arranged to transfer additional classified information in his possession to the purported Russian agent at Union Station in downtown Denver. Using a laptop computer and the instructions provided by the FBI online covert employee, Dalke transferred five files, four of which contained Top Secret information. The other file was a letter, which begins (In Russian & Cyrillic characters) "My friends!" and states, in part, "I am very happy to finally provide this information to you… I look forward to our friendship and shared benefit. Please let me know if there are desired documents to find and I will try when I return to my main office." The FBI arrested Dalke on Sept. 28, 2023, moments after he transmitted the files. (Source)

NSA Employee Charged For Willful Transmission And Retention Classified Information Using His Personal E-Mail Address 13 Times - March 31, 2022

Mark Unkenholz is as an employee of the National Security Agency (NSA). He held a Top Secret / SCI clearance.

On 13 occasions between Feb. 14, 2018 and June 1, 2020, Unkenholz willfully transmitted classified information to another person who was not entitled to receive it. The information transmitted was classified at the Secret and Top Secret / SCI levels. Unkenholz transmitted the classified information using his personal email address to the other person's private company email addresses. The person receiving the information held a Top Secret / SCI clearance from April 2016 until approximately June 2019. (Source)

NSA Subcontractor Employee Sentenced To Prison For Billing Government For 1,200 Hours Not Worked - September 2, 2021

According to her plea agreement, Company A was a subcontractor for Company B, providing employees that performed national security duties for the Department of Defense (DOD). From January 2017 until March 2019, Melissa Heyer worked for Company A, but was assigned on a day-to-day basis to work for the DOD on national security matters at the National Security Agency (NSA), in Fort Meade, Maryland.

From January 2017 through March 2019, Heyer used a badge reader to gain access to the SCIF. Heyer falsely represented to her employer that she had been working at the NSA SCIF when she was actually elsewhere. Heyer caused false claims to be submitted to the DOD that resulted in the government paying more than $100,000 for hours Heyer were not entitled to In total, as result Heyer knowingly caused the government to be billed for more than 1,200 hours of her time when she had actually not worked. (Source)

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

WHO CAN BE AN INSIDER THREAT TO AN ORGANIZATION?

- ☐ Outsider With Connections To Insider (Relationship, Marriage Problems, Restraining Orders, Etc.)
- ☐ Employee Threats (To Include; Contractor / Trusted Business Partner)
- ☐ Disgruntled Employees Transforming To Insider Threats / Job Jumpers
- ☐ Opportunist Employees
- ☐ Any Individual That Has Authorized Access Or Gains Unauthorized Access To An Organization Assets: Facilities, Employees, Financial Assets, Data, Computer Systems, Networks, And Whose Actions Could Negatively Impact An The Organizations Assets
- ☐ Foreign Nation State Sponsored Insider Threat (Recruitment Of Insiders For Nation State Objectives)

TYPES OF INSIDER THREATS INCIDENTS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Organization With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Organizational Policy
- ☐ Employee Stealing Their Employers Money To Fund Their Personal Business
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Geopolitical Risks / Divided Loyalty Or Allegiance To U.S. / Terrorism

INSIDER THREAT BEHAVIORAL INDICATORS

The links below provide the many different types of behavioral indicators that an employee may exhibit that should be of concern to an IRM Program.

Behavioral Indicators Of Concern For Insider Threat Programs Part 1

Behavioral Indicators Of Concern For Insider Threat Programs Part 2

Behavioral Indicators Of Concern For Insider Threat Programs Part 3

Using External Data Sources For Insider Threat Detection & Mitigation

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls. While the report is not focused on the U.S. Government, it provides a lot of useful information.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Has the Chief Information Officer or the Insider Threat Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

Key Findings From Report / Infographic

Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic

Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic

Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERE THE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic

Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic

Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS FRAUD MITIGATION RESOURCES

Fraud Risk Schemes Assessment Guide
Fraud Risk Management Scorecards
Other Tools

DEPARTMENT OF DEFENSE FRAUD MITIGATION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators
Fraud Red Flags & Indicators
Comprehensive List Of Fraud Indicators

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**6,000+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS REPORT FOR THE DEPARTMENT OF DEFENSE (DOD) / 2024

The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. This is very evident in the research that has been conducted by the NITSIG and the ITDG since 2014, and published in the Insider Threat Incidents Reports that are produced monthly.

While some employees may display behavioral indicators of concerns, some may not. Other employees are apparently motivated by human greed, the need for more money, or the opportunity to live a lifestyle of luxury at the expense of the DoD. Perpetrators have used DoD money for: Investment Ventures, To Pay Debts, Jewelry, Clothing, Vehicles, Real Estate, Vacations and more. Download Report / No Registration Required

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector) Download Report / No Registration Required

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER / X

Updated Daily

https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The NITSIG Provides IRM Guidance And Training To The Membership And Others On;

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

NITSIG IRM Resources

Posted on the NITSIG website are various documents, resources and training that will assist organizations with their IRM / IRM Program efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.

https://www.nationalinsiderthreatsig.org/aboutnitsig.html

NATIONAL INSIDER THREAT SPECIAL INTEREST GROUP

INSIDER THREAT SYMPOSIUM & EXPO (TM)

March 4, 2025

Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland

Are you looking for expert guidance from Insider Risk Management (IRM) Program Experts for developing, managing, evaluating or optimizing a program?

The NITSIG will be holding the Insider Threat Symposium & Expo (ITS&E) on March 4, 2025, at the Johns Hopkins University Applied Physics Laboratory (JHU-APL, Laurel, Maryland), in the Kossiakoff Center. The event runs from 8AM to 5PM. This will be the 5th ITS&E held.

This year's event will feature subject matter experts with real world experience in IRM Programs and an interactive breakout panel that will discuss a variety of IRM topics.

Confirmed Speakers

- Larry Knutsen / Retired CIA Insider Threat Program Manager
- Shawn Thompson / IRM Program Legal Expert (Former DoD Senior Litigation Attorney, FBI Assistant General Counsel)
- Todd Masse & Bill Smith / JHU- APL IRM Program
- Kevin Burton / Vice President, IRM Lead At Synchrony Financial
- Frank Greitzer, PhD / Chief Behavioral Scientist For Cogility Software
- Zak Lewis / EchoMark Insider Threat Leak Detection Tool
- Cyber Security & Infrastructure Security Agency (CISA)
- Deidra Bass / Director, Navy Insider Threat Program
- Department Of Defense Insider Threat Management Analysis Center (DITMAC)
- And More...

More Information Can Be Found On This Link:
www.insiderthreatsymposium.org

The ITS&E brings together individuals from the U.S. Government, Department Of Defense, Intelligence Community Agencies, Defense Contractors, Critical Infrastructure, Law Enforcement, Universities and the private sector companies, for a 1 day event that features expert speakers, engaging and interactive panel discussions, vendor technologies and solutions, and networking with IRM practitioners.

The link below provides a complete overview of the NITSIG, advisory board members and the very positive comments (Page 19) from our membership and other individuals that have attended NITSIG meetings, workshops and ITS&E events.
https://www.nationalinsiderthreatsig.org/pdfs/NITSIG%20Overview%20With%20Comments.pdf

ITS&E Registration (Cost: $69 / Includes Continental Breakfast / Lunch)
https://www.eventbrite.com/e/insider-threat-symposium-expo-3-4-25-registration-tickets-1078741698459

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates, as well as attended our Insider Threat Investigations - Analysis Training Course and other training courses.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and IRM Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive IRM.

ITDG training and consulting services will empower individuals that manage or support IRM Programs, with the comprehensive knowledge, tools and a unified and holistic approach to identify, prevent and mitigate Insider Risks / Threats.

IRM PROGRAM TRAINING & CONSULTING SERVICES OFFERED
Conducted Via Classroom / Onsite / Web Based
TRAINING

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training Course & Workshop / Table Top Exercises For C-Suite, Insider Risk Program Manager / Working Group
- ✓ IRM Program Development, Management & Optimization Training Course
- ✓ IRM Program Evaluation & Optimization Training Course
- ✓ Insider Threat Investigations & Analysis Training Course
- ✓ Insider Threat Awareness Training For Employees'

CONSULTING SERVICES

- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration / Red Team Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of 675 Clients:
White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more.
(Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Members
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org