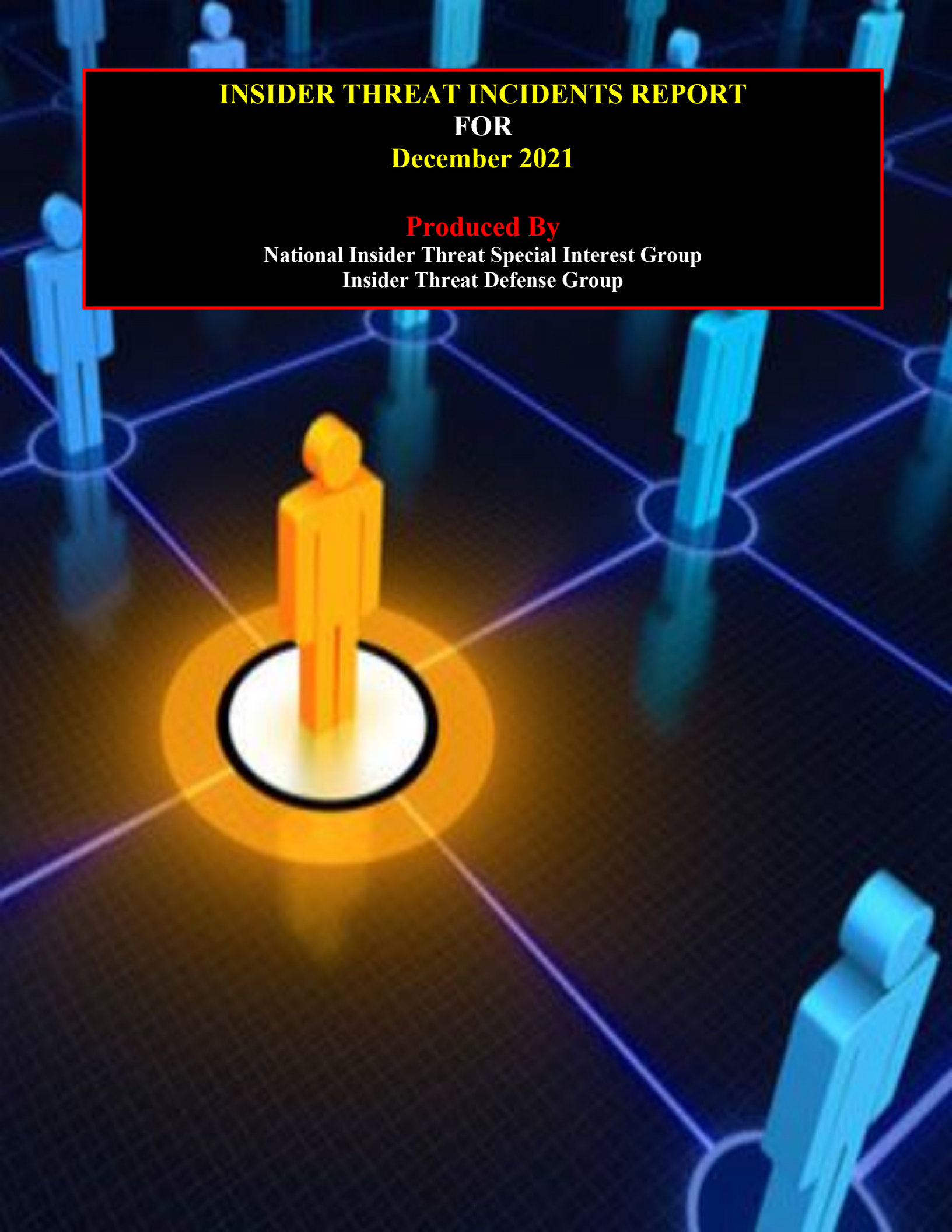

INSIDER THREAT INCIDENTS REPORT
FOR
December 2021

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees who sit behind firewalls or telework through firewalls. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **3,200+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees.

According to the Association of Certified Fraud Examiners 2020 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to significant underreporting on the Insider Threat problem.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 25 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

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 CC2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees Transforming To Insider Threats
- ☐ Theft Of Organizations Assets
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, 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 Employer With Fake Invoices
- ☐ Employees Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ 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
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports, Aviation / Airline Industry (Pilots, Flight Attendants)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials)
- ☐ And Others

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction (Downtime)
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead

Reputation Impact

- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ Employees Loose Jobs / Company Goes Out Of Business

INSIDER THREAT INCIDENTS
FOR DECEMBER 2021

U.S. GOVERNMENT

Former 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 traveling 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)

4 U.S. Postal Service Mail Carriers / 9 Other Suspects Are Accused Of Stealing Credit Cards From Mail As Part Of $750,000 Identity Theft Ring - December 8, 2021

4 U.S. Postal Service (USPS) mail carriers, including 3 from New York City are accused of stealing credit cards from the mail as part of a $750,000 identity theft ring.

The postal workers and 9 other suspects were indicted in Manhattan Supreme Court on conspiracy, grand larceny and a litany of other charges over the scheme that took place between January 2017 and August 2019, according to the Manhattan District Attorney's Office.

The USPS employees, who were recruited by ringleader Michael Richards, of Manhattan, allegedly swiped over 1,000 credit cards that were then used by another defendant to buy high-end goods at luxury retailers. Richards paid the mail carriers different amounts depending on how well the cards they stole performed, the DA's office said in a press release. (Source)

Former U.S. Postal Service 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)

U.S. Postal 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, which 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)

Former U.S. Postal Service 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)

Former U.S. Postal Service 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)

Former Sandia National Laboratories Employee Sentenced To Prison Misuse Of Government Credit Card For 4 Years - December 10, 2021

Joshua Cordova admitted that during the period from September 2014 through September 2018 he fraudulently used the government-funded procurement cards that had been entrusted to him to purchase items for the personal use of himself, his family, and his associates. These items included: jewelry; watches, clothing; shoes; golf clubs and golf accessories; exercise equipment; toys; barber equipment, furnishings and supplies; building materials; and home appliances.

To conceal the fraudulent use of his purchasing card, Cordova made misrepresentations and false statements, claiming in his monthly reconciliation reports the purchases were legitimate items.

For example, in August 2017, Cordova purchased a diamond ring for $944 from Amazon.com that was shipped to his home. In his monthly report, he represented the purchase as "2 carbon fiber Manfredo 510 tripods." (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Pentagon Report Finds About 100 U.S Troops Involved In Extremist Activities - December 20, 2021

We believe that less than 100, or about 100, active duty or reserve component members of the military participated in prohibited extremist activities," Pentagon press secretary John Kirby said during recent press briefing.

Kirby's comments come after the Department of Defense Monday released its report, "Countering Extremist Activities," which was ordered by Defense Secretary Lloyd Austin earlier this year after it was found many of the participants in the Jan. 6 Capitol riot were active military or veterans.

The report outlines next steps to combat extremist activity in the military, detailing certain extremist activities, including advocating terrorism or supporting the overthrow of the government, that are prohibited for service members to engage in. (Source)

Former Defense Contractor Employee Arrested For Attempted Espionage - December 16, 2021

John Rowe attempted to provide classified national defense information to the Russian government. Rowe, who is originally from Massachusetts, was employed for nearly 40 years as a test engineer for multiple cleared defense contractors. In connection with his employment, Rowe held various national security clearances from SECRET to TOP SECRET / SCI. He worked on matters relating to the U.S. Air Force's aerospace technology.

After committing a number of security violations and revealing a fervent interest in Russian affairs, including whether he could obtain a security clearance from the Russian government, Rowe was identified as a potential insider threat and terminated from employment.

The FBI began an undercover operation to determine Rowe's willingness to communicate classified information to a foreign government. In March 2020, Rowe met with an undercover FBI employee who posed as an agent of the Russian government. Over the course of the next eight months, Rowe exchanged over 300 emails with the purported Russian agent, confirming his willingness to work for the Russian government and discussing his knowledge of classified information relating to U.S. national security and military interests. Rowe disclosed national defense information classified as SECRET that concerned specific operating details of the electronic countermeasure systems used by U.S. military fighter jets. (Source)

Former Veterans Affairs Employee (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 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)

Air Force Police Officer Charged With $250,000+ COVID Unemployment Insurance Fraud - December 10, 2021
Trevon Miller, 28, wa a Military Police Officer at Edwards Air Force Base

Trevsob Miller is charged with mail fraud for submitting fraudulent unemployment insurance claims in over 30 states during the ongoing COVID-19 pandemic. From at least April 2020 through June 2020, Miller submitted the fraudulent claims using his former identity of Trevon Rodney and told the state workforce agencies that administer the unemployment insurance system that he was unemployed when he was enlisted in the Air Force the whole time. In 2016, Miller had legally changed his last name from Rodney before he joined the Air Force. The state workforce agencies and the United States were subject to a potential loss of more than $250,000. Miller used the money for his own benefit, including making cash withdrawals. (Source)

Former Ft. Bragg Employee Pleads Guilty To Bribery Over 8 Years - December 7, 2021
Edward Wade Crisco was a flooring technician assigned to the Operations and Maintenance Division, Directorate of Public Works (DPW) at Fort Bragg, NC.

From 2011 into 2019, Crisco received bribes ranging from $20 to $100 per DMO from various vendors contracting with DPW, Ft. Bragg, to request contracts be assigned to those specific vendors and to approve and sign off favorably on their work once completed. (Source)

Former Veterans Benefits Administration Employee Sentenced To Prison Defrauding The Veterans Administration Of $183,000+ Over 5 Years For Personal Use - 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)

Former U.S. 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)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former College Track And Field Coach Charged With Wire Fraud, Cyberstalking, Conspiracy And Computer Fraud Charges - December 2, 2021

Steve Waithe is a former track and field coach.

He is charged in connection with a scheme to trick women across the country into sending him nude or semi-nude photos using more than a dozen sham social media and email accounts. Waithe cyberstalked one female student-athlete and orchestrated a scheme to gain unauthorized access to a victim's Snapchat account. (Source)

Former Puerto Rico Mayor Pleads Guilty To Accepting Bribes From Contractor In Exchange For Awarding Millions In Contracts - December 2, 2021

Felix Delgado-Montalvo was the Mayor of in the municipality of Cataño.

Delgado-Montalvo unjustly enriched himself by accepting bribes, including cash payments from a particular person, whose business would then benefit by being rewarded contracts, including a contract worth nearly $50,000. Delgado-Montalvo agreed to forfeit $105,820 as proceeds of his illegal conduct.

Mario Villegas-Vargas who owned an asphalt and paving company in Puerto Rico, was arrested for allegedly paying kickbacks and bribes to Delgado-Montalvo in exchange for valuable municipal contracts. Beginning in or around June 2017, Villegas-Vargas paid kickbacks and bribes in exchange for Delgado-Montalvo exerting his influence on officials in Cataño, resulting in Villegas-Vargas's business receiving over $9.9 million in municipal contracts.(Source)

Former University Of Guam Professor And Co-Conspirators Sentenced To Prison For $200,000+ Bid-Rigging Scheme - December 9, 2021

From November 2014 to June 2015, Thomas Marler conspired with John Lawrence and Jayanika Lawrence to rig bids for federally-funded project work pursuant to cooperative agreements between the federal government and the University of Guam (UOG).

During this time, Marler was a Professor at the University Of Guam (UOG) Professor as well as the Principal Investigator for certain federally-funded cooperative agreements where his responsibilities included bidding out and awarding project work in compliance with UOG's procurement process.

However, instead of soliciting bids from the Guam community, Marler produced fictitious bids in order to make the procurement process appear legitimate and awarded the project work to Isla Paraiso, a company controlled by Marler, and to Sansar Consulting, a company owned by Jayanika Lawrence and operated with the help of John Lawrence, Marler's longtime friend and associate. During the time of the conspiracy, the defendants fraudulently obtained over $200,000 in project work. (Source)

Former Program Coordinator For Office Of The Courts Sentenced To Prison For $70,000+ Contract Bribery Scheme - December 10, 2021

Jean-Joseph Saulnerond engaged in a long-running scheme to defraud the Administrative Office of the Courts (AOC) for the Commonwealth of Kentucky. He worked as a Languages Other Than Spanish (LOTS) Program Coordinator. As the LOTS Program Coordinator,

Saulnerond was responsible for scheduling foreign language interpreters for court hearings within the Commonwealth of Kentucky and had the authority to award contracts and assign jobs for interpretation services.

Saulnerond solicited and received bribes and kickbacks in exchange for awarding interpretation contacts and assigning jobs to provide interpretation services for the AOC to individual interpreters and a language services company. At times, he refused to award interpretation contracts and assign jobs to individuals and companies if they did not agree to pay him a bribe or kickback. As part of the scheme, interpreters inflated the hours worked on contracts with the AOC in order to be paid additional money to kickback to Saulnerond out of the contracts' proceeds. Between 2011 and 2018, Saulnerond solicited and received over $70,000 in bribes and kickbacks from contractors. (Source)

High-Profile Houston Mayor & Judge Face Corruption Allegations Involving Contract Awards - December 13, 2021

Houston Mayor Sylvester Turner and Harris County Judge Lina Hidalgo are each battling similar but separate controversies involving millions of dollars in government contracts awarded to politically connected individuals.

Hidalgo has faced intense scrutiny over an $11 million vaccine outreach contract to Elevate Strategies, which is run by Felicity Pereyra, a Democratic political insider with ties to the county commissioners court. Pereyra's company was a one-woman operation until recently and only had existed for two years before being awarded the contract. Pereyra's company was awarded the contract over UT Health, one of the city's major hospitals, and the "deciders" for the contract all answered directly to Hidalgo without input from the commissioners' panel. A mix of industry experts and county officials stated that Elevate Strategies did not even meet the basic requirements to engage in an endeavor of this scope. Additionally, the experts and officials said that there was no way that Elevate Strategies could have met the strict financial requirements for bidding on county contracts. Hidalgo canceled the deal amid scrutiny but thousands of dollars were still paid to Elevate Strategies by the county as the arrangement imploded.

Turner made local headlines when he was accused of corruption by former Houston Housing and Community Development Director Tom McCasland regarding a $15 million housing contract the mayor allegedly moved to award to a "co-developer" firm – the Harbor Venture Group – where his former law partner, Barry Barnes, is in charge. (Source)

Former Mayor Pleads Guilty To Accepting $5,000 Monthly Bribe Payments Over 5 Years In Exchange For 10 Year Contract - December 16, 2021

The former mayor of Aguas Buenas, Puerto Rico, Luis Arroyo-Chiqués, pleaded guilty to engaging in a bribery scheme in which he received cash payments in exchange for awarding a 10-year municipal contract for waste collection services.

Arroyo-Chiqués was the mayor and highest-ranking government official in the municipality of Aguas Buenas from 2005 until 2016. In 2016, Arroyo-Chiqués negotiated a waste collection contract for Company A. In exchange for the 10-year waste collection contract, Arroyo-Chiqués received a monthly $5,000 kickback payment. This payment was made in cash every month beginning in 2016 and continued even after Arroyo-Chiqués left office in December 2016. The last payment occurred in June of 2021. (Source)

Former Harvard University Professor Convicted For Concealing His Affiliation China's Thousand Talents Program - December 21, 2021

Dr. Charles Lieber who was the former Chair of Harvard University's Chemistry and Chemical Biology Department was convicted by a federal jury in connection with lying to federal authorities about his affiliation with the People's Republic of China's Thousand Talents Program and the Wuhan University of Technology (WUT) in Wuhan, China, as well as failing to report income he received from WUT.

Lieber served as the Principal Investigator of the Lieber Research Group at Harvard University, which received more than $15 million in federal research grants between 2008 and 2019. Unbeknownst to his employer, Harvard University, Lieber became a "Strategic Scientist" at WUT and, later, a contractual participant in China's Thousand Talents Plan from at least 2012 through 2015. China's Thousand Talents Plan is one of the most prominent talent recruitment plans designed to attract, recruit and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security.

Under the terms of Lieber's three-year Thousand Talents contract, WUT paid Lieber a salary of up to $50,000 per month, living expenses of up to $150,000 and awarded him more than $1.5 million to establish a research lab at WUT. In 2018 and 2019, Lieber lied to federal authorities about his involvement in the Thousand Talents Plan and his affiliation with WUT. (Source)

Community College District Vice Chancellor Charged With Embezzlement - December 21, 2021

Jose Nunez served as the Vice Chancellor of facilities for 21 years at the district that oversees Skyline College, Cañada College and the College of San Mateo, Califorina.

Nunez has been charged with 15 felonies, including embezzlement and perjury, county prosecutors.

Prosecutors allege that the embezzlement occurred in 2013 and 2014 related to the awarding of a contract for a solar photovoltaic project at Cañada College, while the perjury charges are for his alleged failure to report various gifts from district vendors over more than a decade.

Nunez also faces two charges of illegally using district resources for political campaign purposes, according to the District Attorney's Office. (Source)

FOREIGN GOVERNMENT ESPIONAGE / LOSS OF CLASSIFIED INFORMATION

Canada's Navy Lost Electronic Storage Devices Containing Top Secret Information - December 9, 2021

Two of Canada's frontline frigates lost electronic storage devices containing classified and top secret data, including electronic warfare material according to security inventories conducted over the last two years.

The devices which were USBs, DVDs and a backup hard drive went missing despite an apparent tightening of security in the wake of a spy scandal almost a decade ago, and a separate internal 2013 board of inquiry which recommended measures to clean up the navy's handling of classified data.

In August 2020 an inventory of the secure data account aboard the ship HMCS Fredericton discovered numerous classified and unclassified (Electronic Warfare] items were missing.

A subsequent search focused on two missing DVDs containing highly sensitive information, including information about threat emitters which are electronic devices to identify and help counter incoming missiles used by the ship's various systems. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

Former Treasurer For Fire Department Union Pleads Guilty To Stealing $200,000+ In Union Funds For Personal Use (Flights, Cruises, Bills, Etc.) - December 2, 2021

Verdine Day was hired by the Detroit Fire Department in 1986. She worked as a firefighter, engineer, and held other positions in the union before she was elected by her peers to Treasurer of the Detroit Fire Department Union (DFFA) in November 2015. She was Treasurer from December 2015 until her retirement from the DFFA and the City of Detroit in September 2019.

During the four years Day was Treasurer of the DFFA, she fraudulently obtained approximately $167,900.00 of union funds by (1) issuing checks in her name and then changing the name of the payee in the Union's Quickbooks software; (2) cashing checks which were voided by her in Quickbooks; (3) writing checks made payable to cash; and (4) withdrawing cash from DFFA bank accounts. Day also fraudulently obtained money by diverting funds intended by the DFFA to be a donation to charity.

Day also used DFFA credit cards as her own personal credit cards while she was Treasurer and after she retired. In total, she charged approximately $49,116.17 in personal expenses using DFFA credit cards. Her purchases on DFFA credit cards included flights, hotel rooms, cruises, car insurance premiums, satellite and cable TV service, national and state parks fees, and furniture. For example, Day used a DFFA union credit card to charge $9,553 for a cruise with Royal Caribbean cruise lines in 2017. Day also used a union credit card to pay for another Royal Caribbean cruise costing $8,975 on the Liberty of the Seas in 2019. She used the union's credit card to pay her bar bill at a casino in Ohio in May 2019 and for a meal at a Bubba Gump Shrimp Co. restaurant in Cozumel, Mexico in 2019. (Source)

Former Bureau Of Prisons Correctional Officer Sentenced To Prison For Accepting $31,000+ In Bribes - December 9, 2021

Casey Covington was employed by the Federal Bureau of Prisons at the Federal Correctional Institution in Butner, North Carolina (FCI Butner) as a correctional officer when he was bribed by three inmates to smuggle contraband into the prison.

From 2019 to 2020, the inmates, Christopher Davis, Antonio Byers, and Robert Huitt, used their contacts outside the prison to pay Covington over $31,000. A review of Covington's financial records revealed the payments which originated from the inmates outside contacts. In exchange, Covington used his position as a correctional officer to smuggle marijuana, cell phones, alcohol and tobacco into FCI Butner and then deliver the contraband to Davis, Byers, and Huitt. In May 2020, authorities at Butner recovered two cell phones and marijuana from the cell shared by Davis and Byers. Later in October 2020, officers recovered a cell phone from inmate Huitt. (Source)

Former Boston Police Dept. Auto Repair Technician Sentenced To Prison For Embezzling $260,000+ In Automotive Supplies - December 15, 2021

Bahram Gharony engaged in a scheme that allegedly defrauded the Boston Police Dept. (BPD) Fleet Management Division of over $260,000 in automotive parts, tools and supplies between June 2017 and September 2020. Gharony used his position to order parts and supplies that he purported were for BPD, but were actually converted and sold to others by Gharony.

In an effort to conceal the scheme, Gharony submitted fraudulent and altered invoices to BPD for the parts, tools and supplies he falsely claimed were ordered for the fleet. Additionally, Gharony purported that he had lawfully purchased the items through a discount available to BPD when selling the items to others. (Source)

Former Baltimore County Police Officer Sentenced To Prison For Identity Theft Of Dead Woman - December 16, 2021

Deandre Ross worked for the Baltimore County Police for 4 years.

Police said Ross was dispatched to investigate a call about a sudden death. The family later filed a theft report for a missing laptop, prompting detectives to begin an investigation that led to criminal charges. Ross pleaded guilty to stealing a dead woman's identity. (Source)

Former Police Detective Charged With Accepting $3,200 In Bribes For Vehicle Fraud Scheme - December 17, 2021

Michael Pacteles while working as a detective with Detroit Police Department (DPD), acepted bribes, including a vehicle and $3,200 in cash, from a towing company operator.

In return, Pacteles agreed to provide favors for the towing company operator. For instance, instead of properly recovering stolen vehicles from the towing company operator's possession, Pacteles removed them from the DPD database that showed they were stolen. Pacteles also agreed to provide the towing company operator with information about vehicles from the Michigan Law Enforcement Information Network (or LEIN), a restricted law enforcement database. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE

Former Medical Practice Administrator Sentenced To Prison For Stealing $270,000 From Medical Practice For Personal Use - December 2, 2021

Joshua Millspaugh worked as the practice administrator for Whitson Vision, P.C., with responsibility for payroll processing, purchasing and bill payment. He was paid an annual salary of over $100,000.

However, less than a year after starting his employment, Millspaugh began using his access to company accounts to divert money to himself. Over the next five years, through over 500 separate transactions, Millspaugh used company money to make personal purchases, pay personal bills, and send extra payroll checks to his bank account, all of which he concealed with false entries in the company's books and fictitious justifications when asked about the expenditures.

Dr. William Whitson, the owner and director of Whitson Vision, advised the Court during the sentencing that the loss suffered by him and his business went beyond the financial damage. He explained how Millspaugh's crimes resulted in long term credit and banking problems for his company, how it significantly lowered the business reputation of his company, and how it left devastating morale problems with other company employees. (Source)

Former Director Of Nursing Services At Rehabilitation Center Produced Fraudulent COVID Vaccine Cards - December 3, 2021

Tammy McDonald, who worked as the Director of Nursing Services at a skilled nursing and rehabilitation center, produced the fraudulent vaccine cards on June 20, 2021, and July 28, 2021.

The indictment further alleges that on October 22, 2021, McDonald was questioned by federal agents with HHS and FBI and lied by stating she did not have access to COVID-19 Vaccination Record Cards and that she never produced a false or inaccurate vaccine card. The indictment alleges this was false because she had personally filled out vaccine cards for individuals she knew had not received a COVID-19 vaccine. (Source)

Former Health Clinic Nurse With Drug Addiction Pleads Guilty To Removing Morphine From Vials And Injecting Herself - December 7, 2021

Between August 2019 and April 2020, Esther Tuller was a Washington-licensed registered nurse employed at the Confluence Health Clinic in Moses Lake, in Washington state. Her position as a nurse provided her with access to medications, including opioid narcotics such as morphine, an opioid derivative commonly prescribed by hospitals and health care facilities to relieve pain.

Tuller used syringes to remove morphine from at least 17 vials, and then ingested that morphine as part of her own opioid addiction. She then replaced the morphine with a saline solution that was essentially salt dissolved in water, and attempted to glue the caps back onto the vials to make them appear intact. Before Tuller was apprehended by law enforcement, at least one Confluence Health patient who was prescribed morphine had to be rushed to the emergency room; that patient continued to be in excruciating pain after receiving only saline from what was supposed to be morphine vials. (Source)

Former Medical Center Nurse Pleads Guilty To Removing Medications From Vials And Injecting Herself - December 8, 2021

Emilee Poteat removed and opened packages containing vials of injectable Hydromorphone from Novant Health Forsyth Medical Center (NHFMC) while employed as a contact nurse in the Clinical Pre / Post Procedure Unit.

From July, 2020 to November, 2020, Poteat removed vials for the purpose of converting and consuming the Hydromorphone by injecting the drug into herself. Poteat then replaced the used vials with tampered vials containing a saline solution. Poteat knew that, in doing so, nurses at NHFMC might unknowingly administer the contents of compromised vials to patients. (Source)

Former Rehabilitation Center Nurse Sentenced To Prison For Substitution Of Hospice Patient Medication - December 20, 201

Marietta Strickland while working as a registered nurse at Dighton Care and Rehabilitation Center in Boston, tampered with three blister card packages of oxycodone prescribed to an 89-year-old hospice patient who suffered from Alzheimer's disease, severe dementia and breast cancer.

To avoid detection, Strickland replaced the stolen oxycodone pills with other prescription drugs disguised to look like oxycodone. As a result of Strickland's tampering, the victim was deprived of her prescribed oxycodone for at least a month and ingested at least 77 unnecessary prescription tablets. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Security Supervisor Sentenced To Prison For $119,000+ Bank Fraud Scheme Using the Stolen Identity Information Of Co-Workers And Job Applicants From His Company - December 9, 2021

From January 2015 to December 2017, Ricardo Carter used stolen names, date of births, and social security numbers of coworkers and job applicants to open fraudulent bank accounts at financial institutions in Maryland, Virginia, and Washington, D.C. He then used the fraudulently opened accounts to execute fraud schemes.

Specifically, once Carter opened a bank account using a stolen identity, he deposited non-sufficient funds checks into the account, then withdrew the value of the check in cash before the check cleared, or transferred the funds into another account, using the money for his personal benefit.

When Carter used a stolen identity to open a credit account, he used the credit card associated with the account for personal expenditures, causing a loss to the bank and adversely affecting the victim's credit score. Carter used the stolen identities to open numerous bank accounts at multiple financial institutions, executing the scheme in multiple jurisdictions, and timing the withdrawal of cash from the deposited checks before those checks could clear.

The judge ordered Carter to forfeit $119,733.94, which are assets derived from or obtained as a result of Carter's illegal activities, and to pay restitution in the full amount of the victims' losses, which is $131,588.24. (Source)

Jury Convicts Former AT&T Retails Sales Employee Of Conspiracy, Fraud And Identity Theft Using Stolen PII Involving Co-Conspirators / AT&T Losses Are $85,000+ - December 10, 2021

Alejandro Williams began working as a retail sales consultant at an AT&T store location in Fayetteville, North Carolina in March 2016. In that capacity, Williams' responsibilities included activating AT&T customer accounts and selling cell phones for those accounts.

In October 2017, Williams was introduced to Anthony Jamison, a resident of Hamlet, North Carolina. Jamison was named as a co-conspirator in the indictment and previously pleaded guilty in this matter.

Between October 2017 and January 2018, Williams and Jamison conspired to establish AT&T cellular accounts with the stolen personal identifying information (PII) of unwitting victims in North Carolina and South Carolina for the purpose of obtaining thousands of dollars' worth of high-end cell phones for resale on the black market.

Jamison would provide Williams with the victim PII, to include Social Security numbers and dates of birth, through text messages and other means. Jamison would then send various recruits into the AT&T store to meet with Williams to act as the "customer" for the surveillance cameras. Thereafter, among other things, Williams would use the stolen victim PII to run hard credit checks, activate lines of service in the victims' names, and, ultimately, issue cell phones to the "customer" for resale by Jamison.

To facilitate the conspiracy, Williams ensured the phones were activated and sold under financing plans that required little or no payment from the "customer" at the point of sale, but which made the victims personally liable for the devices without their knowledge. Many victims only learned of the scheme when they discovered AT&T bills addressed to them in the mail. During one particular transaction, for example, Williams used the stolen personal identifiers of a North Carolina victim to issue nine iPhone devices, valued at over $8,500, on installment plans created using that victim's name and credit history. In total, the associated losses to AT&T as a result of the scheme, including phones and accessories, was in excess of $85,000.00. (Source)

BANKING / FINANCIAL INSTITUTIONS

4 Former Executives Of Financial Institutions Plead Guilty To Fraud Scheme That Caused $4.5 Million+ In Losses To Small Business Administration - December 1, 2021

3 former executives of Valley Bank, a defunct financial institution based in Moline, Illinois, and the President of Vital Financial Services (Vital Financial), a lending service provider, have pleaded guilty to scheming to defraud the Small Business Administration (SBA) in connection with its programs to guarantee loans made to small businesses.

Michael Slater, former President and Founder of Vital Financial, **Larry Henson**, former President and Chairman of Valley Bank, **Andrew Erpelding** former Vice President and Regional Manager of Valley Bank and **Susan McLaughlin** former Vice President for Credit Administration of Valley Bank conspired to and fraudulently obtained loan guarantees from the SBA on behalf of Valley Bank borrowers, knowing that the loans did not meet SBA's guidelines and requirements for the guarantees. They did so by, among other things, altering loan payment histories, renaming businesses, and hiding the fact that borrowers had previously defaulted on loans.

When the fraudulently guaranteed loans defaulted, the defendants caused the submission of reimbursement requests to the SBA to purchase the defaulted loans from investors and lending institutions, thereby shifting the majority of losses on the ineligible loans to the SBA. In all, the defendants attempted to obtain guarantees on over $14 million in loans, were successful in obtaining guarantees on over $9 million in loans, and caused the SBA losses of over $4.5 million. (Source)

CEO Of Credit Union Pleads Guilty To Charges Forcing Credit Union To Go Out Of Business / Had Help From CFO Who Embezzled $1.5 Million - December 14, 2021

Helen Godfrey-Smith was employed by the Shreveport Federal Credit Union (SFCU) from 1983 to 2017 and during much of that time was employed as the Chief Executive Officer (CEO) of the SFCU.

In October 2016, the SFCU, through Godfrey-Smith, entered into an agreement with the United States Department of the Treasury to buy back certain securities that were part of the Department's Troubled Asset Relief Program (TARP). As part of that process, on December 27, 2016, Godfrey-Smith signed and submitted to the United States Department of the Treasury an Officer's Certificate which certified that all conditions precedent to the closing had been satisfied.

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury and the NCUA, SFCU was in a financial crisis.

From 2015 through 2017, another individual who was the Chief Financial Officer of SFCU (Individual 1), had been falsifying call reports to the NCUA which included millions of dollars in fictitious fee income. In addition, she was creating fictitious entries in the banks records to support the false call reports. This created the illusion that SFCU was profitable when, in fact, the bank was failing. In addition, Individual 1, embezzled approximately $1.5 million from the credit union.

In the Spring of 2017, the SFCU failed. It was taken over by regulators from the NCUA and placed into a conservatorship. An investigation by the NCUA revealed that SFCU had amassed in excess of $10 million in losses by December 2016. (Source)

3 Former Bank Board Of Directors Charged With Criminal Conspiracies At Failed Chicago Bank - December 8, 2021

An ongoing federal investigation into the failure of Washington Federal Bank for Savings in Chicago has resulted in criminal charges against 3 former members of the bank's Board of Directors who allegedly conspired to obstruct regulators and falsify bank records.

Washington Federal was closed in December 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. Several former Washington Federal employees, including the bank's Chief Financial Officer and Treasurer, were previously indicted for allegedly conspiring with an Illinois attorney and other individuals to embezzle money from the bank. A federal grand jury returned a 37 count superseding indictment that added four new defendants, including the three former Board members, bringing the total number of charged defendants to fourteen. (Source)

Former Credit Manager Sentenced To Prison For Embezzling $631,000 Over 11 Years - December 16, 2021

Johnnie Harrell served as branch manager of a credit union. From 2008 to 2019, Harrell exploited his position to steal and embezzle at least $631,838 in funds belonging to the credit union and its customers. Among Harrell's victims were individuals convinced by Harrell to rollover existing retirement accounts into annuities. Harrell never purchased the annuities, but instead converted the funds to personal use. Harrell prepared fraudulent annuity account statements that were periodically presented to victims to preclude detection of the theft. (Source)

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD/ BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING

Criminals Have Stolen Nearly $100 BILLION In COVID Relief Funds According To The Secret Service Employees Of U.S. Government & Businesses Involved - December 21, 2021

The stolen funds were diverted by fraudsters from the Small Business Administration's Paycheck Protection Program, the Economic Injury Disaster Loan program and a another program.

Recovered funds include more than $400 million from PayPal and Green Dot Corporation. The government has shelled out about $3.5 trillion in Covid relief money since early 2020, when the pandemic began.

More than $2.3 billion in stolen funds have been recovered so far, resulting in the arrest of more than 100 suspects who span the spectrum from individuals to organized groups.

I've been in law enforcement for over 29 years and worked some complex fraud investigations for 20 plus years, and I've never seen something at this scale," said Assistant Special Agent in Charge Roy Dotson, who was named to the new role at the agency. (Source)

NOTE:

Research by the National Insider Threat Special Interest Group has indicated that some of the fraudsters were employees working for either the U. S. Government or businesses that created shell companies to collect the Covid relief funds.

Former Employee Charged With Stealing Confidential Data And Extorting Company For $2 Million Of Ransom While Posing As Anonymous Attacker - December 1, 2021

Nickolas Sharp was charged for secretly stealing gigabytes of confidential files from a New York-based technology company where he was employed, and then, while purportedly working to remediate the security breach he created, extorting the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by a significant drop in the company's share price associated with the loss of billions of dollars in its market capitalization. (Source)

Former Food Company Human Resources Manager Sentenced To Prison For $69,000+ Payroll And COVID-19 Testing Scheme To Purchase Speedboat - December 2, 2021

Douglas Wold worked as the Human Resources Manager for Fry Foods, Inc. in Ontario, Oregon.

Beginning in at least May 2020 and continuing through August 2020, Wold committed wire fraud by submitting fraudulent payroll requests for individuals who never worked at Fry Foods or who no longer worked at Fry Foods at the time of the payroll requests. Payroll checks were processed based on Wold's requests. Wold then deposited these fraudulent payroll checks into his own bank accounts.

Wold committed mail fraud with respect to a COVID-19 testing program at Fry Foods. Wold issued a fraudulent invoice to Fry Foods in the name of his business, Hala Lallo Health, for $39,995 when, in fact, the testing was provided by another entity and at a greatly lower cost. When Fry Foods paid Hala Lallo Health for the testing, Wold deposited the funds into a bank account he controlled and did not pay the health care provider that actually conducted the testing.

Wold transfered $69,116.48 in proceeds from his frauds for the purchase a speedboat and trailer, which the Government has since recovered. (Source)

Former Office Manager / Bookkeeper Sentenced To Prison For $1.7 Million Bank Fraud Scheme For 7 Years - December 1, 2021

From January 2014 through March 2019, Tanny Martinez served as an office manager and bookkeeper for a New Jersey based company.

Beginning in January 2014, Martinez used her position at the company to issue fraudulent checks made payable to herself or cash and forged the signature of her manager on the fraudulent company checks.

Martinez converted the fraudulent company checks into cash at bank branches in New Jersey. The scheme allowed Martinez to embezzle hundreds of thousands of dollars every year for more than half a decade, resulting in approximately $1.78 million in losses. (Source)

President Of Non-Profit Organization Pleads Guilty To Stealing $130,000+ Over 4 Years For Gambling - December 2, 2021

Walter Greenhowe admitted that from 2014 to 2018 while President of the nonprofit, he engaged in a scheme to defraud the organization of approximately $130,349.07.

Greenhowe used the nonprofit's debit card to obtain cash for his personal use from ATMs at various roadside gaming parlors. Greenhowe admitted that these transactions were unauthorized and unapproved by the nonprofit. Greenhowe often made these withdrawals late at night or early in the morning and removed cash multiple times a night. (Source)

Former Employee For Medical Billing Service Pleads Guilty To Healthcare Fraud, Aggravated Identity Theft - Use Funds For Personal Use - December 3, 2021

Joshua Maywalt was a medical biller at a company that furnished credentialing and medical billing services to its medical provider clients.

Maywalt abused his role as a medical biller by wrongfully accessing and utilizing the company's patient information and Physicians name and identification number, and using those to submit false and fraudulent claims to a Florida Medicaid HMO for medical services purportedly, but not actually, rendered by the Physician. Maywalt then altered the "pay to" information associated with those claims so that the payments for the fictitious medical services were sent to bank accounts under his control. (Source)

Former H&R Block Employee Accused Of Stealing Unemployment Benefits From Customers (Repeat Offender) - December 3, 2021

Russell Mays started this year as an employee for H&R Block. But it wasn't long before one customer noticed that right after her tax appointment with Mays, her unemployment benefits stopped.

Mays had asked the customer for her login information. Mays was the only person who knew the customer account info. More than $1,400 is missing in unemployment benefits from the customer account up. When detectives started digging deeper with they found the a Wells Fargo bank account tied to Mays account that was bringing more than $700 in unemployment funds from another person.

Court records show this isn't Mays' first fraud charge or his second. A year after a 2018 indictment for credit card and identity theft, Mays was convicted of forgery when applying for a job at Los Poblanos.

When his application was flagged for a criminal record, an employee says he claimed he was a victim of identity theft and produced falsified court documents that seemed to misuse two legal terms. After a court confirmed the documents were false, Los Poblanos reported Mays to police.

So how was May able to pass a background check with H&R Block? Mays used his mom's social security number, which was linked to no known criminal record. (Source)

Former Office Manager Sentenced To Prison for Defrauding Her Employer of $149,000+ For Personal Use & Family - December 6, 2021

Yvette Fontenot was employed as an Office Manager at Periodontics Associates in Lafayette, Louisiana. In that position, Fontenot was authorized to use certain credit cards for business expenses, as well as certain business accounts to pay the balances of those credit cards and other business expenses.

From November 2008 until August 2016, Fontenot used several of the business credit cards issued to Periodontics Associates for personal expenses for herself and her family. Fontenot knew that these credit cards were obtained and authorized for business use only and she knew that other business accounts would be used to pay the balances of the credit card accounts.

Fontenot used the business funds to pay her credit card balances and personal expenses through business checks prepared by Fontenot herself. The amount of loss suffered by the company as identified in the criminal proceedings was $149,461.48. (Source)

Former Office Manager Pleads Guilty To Fraudulently Obtaining $1 Million+ From Employer Over 8 Years For Personal Use - December 6, 2021

Tamy Moore was an office manager for a company that made custom components for a variety of industries.

Moore admitted that from 2012 to 2020, she fraudulently obtained more than $1 million from the company. Moore issued company checks to herself and her husband's business from the company's account, forged the signature of the company's owner on checks, deposited the checks into her personal bank account and her husband's business account for her personal benefit, and then initiated online transfers to move the money.

Moore concealed these transactions by making it appear as though the checks were for legitimate business purposes and by deleting the company's records of the forged checks.

Moore is required to pay restitution to the company in the amount of $1,115,629. (Source)

2 Former Employees Of Mechanical Contractors Charged With Conspiracy & Fraud Offenses For Personal Gain - December 7, 2021

William Sacco was a project manager for a Massachusetts-based mechanical contractor. From June 2014 through December 2018, Sacco conspired to defraud his employer and the owners of certain projects he managed by inflating change orders on the projects. As part of the conspiracy, a co-conspirator subcontractor made payments to Sacco and also for Sacco's benefit, including payments for Sacco's children's college tuition, a graduation party, a Mac laptop, airline tickets, hotels and Sacco's rent. Sacco and the co-conspirator submitted inflated change orders to Sacco's employer to offset some of the costs of the payments the co-conspirator made to Sacco.

Don Richards was a senior project manager at a Massachusetts-based mechanical contractor. From November 2014 through February 2018, Richards also conspired to defraud his employer and project owners by inflating change orders on certain projects he was managing. As part of this separate conspiracy, a co-conspirator subcontractor made payments to Richards and also for Richards's benefit, including gift cards and funds for a golf club membership. Richards and the co-conspirator submitted inflated change orders to Richards's employer to offset some of the costs of the payments the co-conspirator made to Richards. (Source)

Former Mortgage Company Loan Officer Admits To Participation In Large-Scale Mortgage Fraud Scheme Involving Co-Conspirators - December 13, 2021

From September 2006 to September 2010, Isaac DePaula and his conspirators engaged in a long-running, large-scale mortgage fraud conspiracy through a mortgage company called Premier Mortgage Services (PMS). The conspirators targeted properties in low-income areas of New Jersey. After recruiting straw buyers, the defendants used a variety of fraudulent documents to make it appear as though the straw buyers possessed far more assets, and earned far more income, than they actually did.

The defendants then submitted these fraudulent documents as part of mortgage loan applications to financial institutions. Relying on these fraudulent documents, financial institutions provided mortgage loans for the subject properties.

The defendants then split the proceeds from the mortgages among themselves and others by using fraudulent settlement statements (HUD-1s), which hid the true sources and destinations of the mortgage funds provided by financial institutions. The defendants made false representations and provided fraudulent documents when, in fact, the straw buyers had no means of paying the mortgages on the subject properties, many of which entered into foreclosure proceedings.

DePaula was a long-time fugitive who was charged by criminal complaint in 2012 and by indictment in 2016. He returned to the United States in March 2020 to face the charges in the indictment. (Source)

Former Store Convenience Manager & Husband Sentenced To Prison For Embezzling $235,000+ Over 5 Years For Personal Use - December 8, 2021

Jeanine Poe was sentenced to 2 years in prison without parole. William Poe was sentenced to five years of probation. Jeanine and William Poe were ordered to pay $235,744 in restitution to the victim of their thefts.

Jeanine Poe was hired by a friend in 2014 to manage two Doc Stop convenience stores, for which she was paid more than $50,000 per year. The owner had little to do with the businesses, except to invest his money into both to ensure their financial success. In 2015, Jeanine Poe told the owner the businesses weren't doing well financially and asked him to invest even more money. The owner invested much of his salary to financially support the businesses.

In October 2019, after the businesses continued to lose money, the owner asked a friend to review the financial affairs of the businesses and learned that Jeanine Poe was embezzling money from his businesses. She had obtained at least seven credit cards in the name of the businesses, conducted transactions on the credit cards, and paid for such transactions with funds from the businesses. All of the credit cards opened by Jeanine Poe had reached their maximum allowable credit limit, and many times were used by Jeanine and William Poe for expenses that were entirely unrelated to the operation of the businesses (such as trips and personal expenses). One of the credit cards was in William Poe's name. The owner also discovered that large amounts of cash were being fraudulently electronically transferred from his businesses' bank account to Jeanine Poe's personal bank account.

The two convenience stores were intended to become the victim's retirement plan and source of future income. However, the business owner had to file for bankruptcy and actually lost one of his two businesses due to the embezzlement scheme. (Source)

Former Cell Phone Store Manager Charged With Cell Phone SIM Swap Scheme - December 9, 2021

In May 2021, Jonathan Katz, who was employed as a manager at a telecommunications store.

He used his managerial credentials to access several customer accounts and swapped the SIM numbers associated with the customers' phone numbers into mobile devices controlled by another individual, enabling this other individual to control the customers' phones and access the customers' electronic accounts. This technique is often used to defeat accounts with two-factor authentication including but not limited to email, social media, and financial accounts. In exchange for the swaps, Katz was paid in Bitcoin, which was traced back to Katz's cryptocurrency account. (Source)

Former Financial Controller Sentenced To Prison For Embezzling $657,000 From 2 Different Employers - December 10, 2021

Christy Bartholomew was employed as a financial controller for a business located in Slidell, Louisiana, and later worked as an office manager for a company located in Kenner, Louisiana.

From 2016 to October of 2019, she embezzled approximately $357,000 from her Slidell employer by several schemes, including unauthorized use of a company credit card. She later did the same thing with her Kenner employer, embezzling approximately $300,000 from November 2019 to February 2020. (Source)

Former Employee Sentenced To Prison For Defrauding Employer Of $2.7+ Million / Spent Money To Pay Mortgage, Buy Luxury Vehicles, Visits To Resorts - December13, 2021

Between February 2019 and September 2020, David Altenburg used his access to his employer's financial accounts to conduct approximately 106 wire transfers and other withdrawals. To execute his scheme, he fraudulently used the name and email address of a firm director to purportedly authorize certain transfers.

In total, he diverted more than $2.7 million to accounts under his control. He used the diverted monies to fund travel; pay down his mortgage; and purchase luxury vehicles, jewelry, clothing, and other items. After learning he was under investigation, he transferred title of his residence to a trust managed by his wife in an effort to prevent its seizure.

Altenburg was also ordered to pay $2,807,080 in restitution to victims of the offenses. (Source)

Former Netflix Vice President Of IT Operations Sentenced To Prison For Receiving $500,00 Bribes And Kickbacks From Companies Contracting With Netflix - December 14, 2021

Michael Kail is the former Vice President of IT Operations at Netflix from. He was convicted of wire fraud, mail fraud, money laundering, pay-to-play bribes and kickbacks from Tech Startups seeking to sell to Netflix.

As Netflix's Vice President of IT Operations, Kail approved the contracts to purchase IT products and services from smaller outside vendor companies and authorized their payments. The evidence demonstrated that Kail accepted bribes in 'kickbacks' from nine tech companies providing products or services to Netflix. In exchange, Kail approved millions of dollars in contracts for goods and services to be provided to Netflix.

Kail ultimately received over $500,000 and stock options from these outside companies. He used his kickback payments to pay personal expenses and to buy a home in Los Gatos, California in the name of a family trust. (Source)

Former Officer Manager Admits To Embezzling $445,000 Over 7 Years To Pay Credit Card Bills - December 21, 2021

Crystal Klatt was employed as an office manager by a property management company located in Hamden.

Clients of the property management company would allow the company access to their bank accounts in order to allow the management company to make payments on behalf of the respective client. Klatt had access to the client's bank accounts as part of her job responsibilities. Between approximately December 2014 and January 2021, Klatt diverted a total of $446,859.82 from the bank accounts of at least 14 clients to pay her personal credit card charges. (Source)

Former Employee For Non-Profit Organization Stole $240,000 To Fund Gambling Addiction - December 21, 2021

According to court documents, the Federal Deposit Insurance Corporation-Office of the Inspector General (FDIC-OIG) initiated an investigation into the financial activities of Trenna Trice in May 2019, following reports of significant casino losses. The investigation into possible sources of income for her casino activity revealed that her sole source of income was working as a teacher for the Muscogee County School District (MCSD). Prior to teaching, she worked for a dental office and she worked as a volunteer campaign coordinator for the Columbus branch of the United Negro College Fund (UNCF) from 2005 – 2017.

Trice was responsible for organizing the annual Columbus Mayor's Masked Ball, UNCF's primary fundraising activity. During the course of the investigation, agents determined that while the larger contribution checks from bigger sponsorship companies had made their way to UNCF, Trice diverted numerous smaller contributions for her own personal use. UNCF ended their relationship with Trice in 2017, following questions regarding financial irregularities that were indicative of embezzlement. It was later discovered that Trice had also been terminated by the dental office following similar allegations.

In total, agents identified 109 checks and 265 credit card transactions fraudulently deposited into Trice's own accounts without authorization. Trice told investigators she had a crippling gambling addiction for the last decade and the money was stolen to fuel her gambling addiction and compensate for her gambling losses. (Source)

Former Amtrak Employee Charged With $26,000 Wire Fraud Scheme Involving 40 Victims - December 23, 2021

Kenya Small was employed by Amtrak as an On-board Services Train Attendant. Small recruited more than 40 victims to purchase spots on a purported June 2019 trip from New Orleans to New York City. Small told the victims that she had booked roundtrip Amtrak train travel for the trip, as well as activities, such as shows and museum visits. In truth, Small had not booked the Amtrak travel or the activities.

When the date of the trip approached, Small told the victims, from whom she had taken a total of approximately $23,000 to $26,000, that Amtrak had canceled the trip because an incident occurred in which one of the trip's passengers assaulted an Amtrak employee and made a bomb threat. In truth, no such incident had occurred.

Small also submitted fraudulent sick benefit claims to the Railroad Retirement Board, a federal agency that provides benefits to Amtrak employees. Small claimed that she was too sick to work when, in truth, she was working another job. (Source)

Former Employee Of Dental Practice Sentenced To Prison For Prescription Fraud And $71,000+ Embezzlement Scheme - December 22, 2021

Lindsey Cox was an employee at a dental practice in St. Albans, Vermont.

Between April and November 2016, Cox conspired with another employee to generate fake prescriptions for controlled substances and forge the signature of a licensed prescriber. Cox and others then filled the fake prescriptions - which typically were for Oxycodone - at several area pharmacies. In total, investigators identified 46 fake prescriptions. In addition, between May 2016 and August 2017, Cox embezzled $71,942.60 from her employer by manipulating and falsifying payment records in the dental practice's billing software. (Source)

Former Restaurants Manager Charged With Embezzling $50,000 - December 23, 2021
Alec Atwood used his position as manager to embezzle from the Gus's Carryout Restaurant. Atwood is charged with one count of embezzling between $20,000 and $50,000. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Bank Tellers Involved With External Co-Conspirators In $300,00 Bank Fraud Conspiracy - December 8, 202
This case arose out of an investigation into schemes to withdraw funds, in the form of checks and cash, from customer accounts at several financial institutions. Organizers of the scheme paid individuals to request bank withdrawals from bank customers' accounts using falsified identification documents in the names of the bank customers.

Bank tellers were also recruited to accept the falsified identification documents without scrutiny and facilitate the withdrawals. The fraudulently obtained funds were then negotiated through accounts at other financial institutions that had been opened in the names of fictitious business entities.

Emelyn Clough opened a bank account in the name of a fictitious business using a counterfeit driver's license and helped recruit a TD Bank teller to participate in this scheme. Thereafter, between June and November 2017, co-conspirators utilized the bank account Clough opened and the bank teller Clough recruited to fraudulently obtain more than $300,000 from customer accounts. (Source)

Former Finance Supervisor Sentenced To Federal Prison For Embezzling Over $900,000 With Help Of Co-Conspirators - December 17, 2021
Between May 2015 and May 2019, Alicia Morgan served as a finance supervisor for her employer. She embezzled $906,109 from the employer by causing the employer to issue approximately 300 checks to Morgan's co-conspirators, whom Morgan falsely and fraudulently represented were vendors that had provided services to the employer and were, therefore, due payment.

Morgan drafted false and fraudulent invoices, check requests, and medical claim forms, indicating that the fake vendors (co-conspirators) had performed services and even met with medical patients. Through creation and submission of these false and fraudulent documents to her employer, Morgan caused the employer to issue payments to her co-conspirators. Morgan then diverted many of these payments into her personal bank account and a bank account she shared with one of the co-conspirators. Morgan used much of the ill-gotten money for her personal expenses. (Source)

THEFT OF COMPANY PROPERTY

Former Amtrak Employee Admits To Obtaining $76,000+ Worth Of Chainsaws / Chainsaw Parts And Selling For Personal Profit Over 8 Years - December 13, 2021
Jose Rodriguez had been an Amtrak employee since October 2007, most recently as a senior engineer and repairman, based out of an Amtrak facility in North Brunswick, New Jersey.

Between March 2012 and July 2020, Rodriguez obtained 114 chainsaws, 122 chainsaw replacement bars, and 222 replacement chains from Amtrak, the total value of which was over $76,000, under the false pretense that this equipment would be used for Amtrak projects. Instead he sold the equipment either on an online auction service or directly to purchasers. Rodriguez used the U.S. Postal Service to mail the stolen chainsaw and chainsaw parts to purchasers throughout the United States, including purchasers in Ohio, Pennsylvania, and West Virginia. (Source)

OTHER FORMS OF INSIDER THREATS

JP Morgan Securities Fined $200 Million By SEC For Letting Senior Manager & Workers Use WhatsApp To Evade Regulators - December 17, 2021

Another example of when senior management contributes to Insider Threats.

The Securities and Exchange Commission stated that JPMorgan Securities agreed to pay $125 million after admitting to "widespread" record-keeping failures in recent years. The Commodity Futures Trading Commission also said Friday that it had fined the bank $75 million for allowing unapproved communications since at least 2015.

SEC officials stated that JP Morgan's failure to preserve those offline conversations violated federal securities law and left the regulator blind to exchanges between the bank and its clients. (Source)

WORKPLACE VIOLENCE

Employee Fired From Job Returns To Work 15 Minutes Later And Kills 2 People / Shooter Killed By Another Employee - October 22, 2021

The investigation revealed that Max Hoskinson, who had been fired that day, had left the grain elevator, but returned. After he was fired, managers there had a meeting to discuss how to proceed after the employee was let go.

When he returned about 15 minutes later, other employees who were unaware that he had been fired didn't think it significant or problematic that he was at the workplace until he walked up to Sandra Nelson's office and shot her dead.

Another employee heard the gunfire and grabbed a gun kept on the premises for pest control and shot the gunman in the chest; he later died. (Source)

TERRORISM

Train Engineer Pleads Guilty To Terrorism Charge For Intentionally Derailing Locomotive Near U.S. Navy Hospital Ship - December 16, 2021

On March 31, 2020, Eduardo Moreno drove a train at high speed and did not slow down near the end of the railroad track. He intentionally derailed the train off the tracks near the United States Naval Ship Mercy, a hospital ship then docked in the Port of Los Angeles.

No one was injured in the incident, and the Mercy was not harmed or damaged, according to court documents. The incident resulted in the train leaking a substantial amount of fuel, which required clean up by fire and other hazardous materials personnel. Moreno caused approximately $700,000 in damages because of the derailment.

Moreno acknowledged that he "did it," saying that he was suspicious of the Mercy and believed it had an alternate purpose related to COVID-19 or a government takeover. Moreno stated that he acted alone and had not pre-planned the attempted attack. (Source)

PREVIOUS INSIDER THREAT INCIDENT REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business (2021)

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA. From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

Former Controller Of Oil & Gas Company Sentenced To Prison For $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data (2021)

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021. Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files. After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

Former Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

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

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**3,200+ 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

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(500+ Incidents)

https://www.insiderthreatdefense.us/category/insider-threat-incidents/

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.

https://www.insiderthreatdefense.us/news/

INSIDER THREAT INCIDENTS COSTING $1 MILLION TO $1 BILLION +

https://www.linkedin.com/post/edit/6696456113925230592/

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

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)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The NITSIG Provides Guidance And Training The Membership And Others On;

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

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

The NITSIG has created a Linked Group for individuals that interested in sharing and gaining in-depth knowledge regarding ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in ITM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

NITSIG Insider Threat Mitigation Resources
Posted on the NITSIG website are various documents, resources and training that will assist organizations with their Insider Threat Program Development / Management and Insider Threat Mitigation efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **640+** organizations. (Client Listing)

Over **875+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over 10+ years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

Our training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org

FTK ENTERPRISE

FOR NETWORK INVESTIGATIONS AND POST-BREACH ANALYSIS

When investigating insider threats, you need to make sure your investigation is quick, covert and able to be completed remotely without alerting the insider. FTK Enterprise enables access to multiple office locations and remote workers across the network, providing deep visibility into data at the endpoint. FTK Enterprise is a quadruple threat as it collects data from Macs, in-network collection, remote endpoints outside of the corporate network and from data sources in the cloud.

Find out more about FTK Enterprise in this recent review from Forensic Focus.

DOWNLOAD

If you'd like to schedule a meeting with an Exterro representative, click here:

GET A DEMO

exterro

[Download FTK Review]
[Get A Demo]
[Exterro Insider Threat Program Checklist]