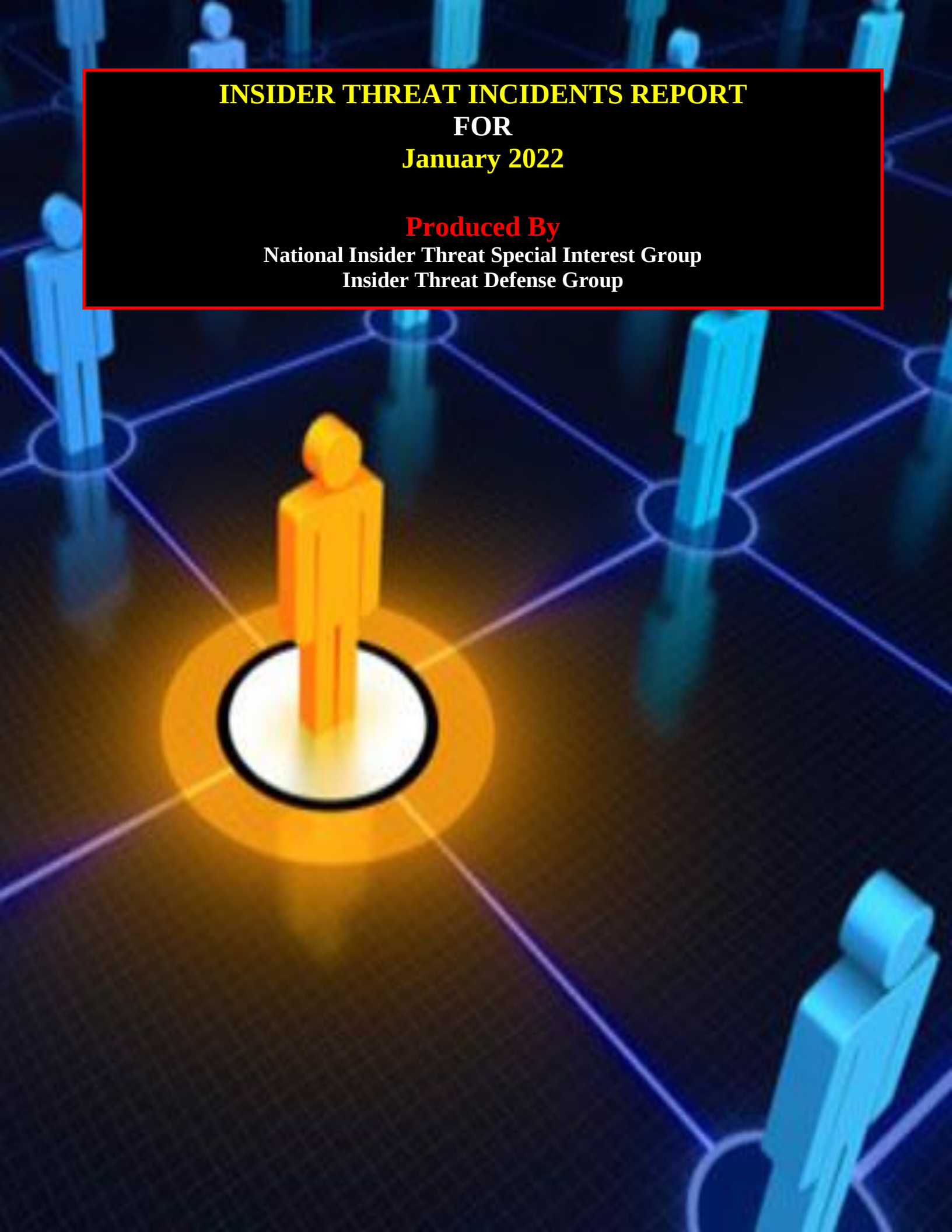

INSIDER THREAT INCIDENTS REPORT
FOR
January 2022

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 **3,300+** 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 19 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 JANUARY 2022

U.S. GOVERNMENT

Former Acting Inspector General For Department of Homeland Security Pleads Guilty To Scheme To Defraud U.S. Government To Help Start His Business - January 14, 2022

Charles K. Edwards executed a scheme to steal confidential and proprietary software from the government.

Edwards worked for DHS-OIG from February 2008 until December 2013, including as Acting Inspector General. Prior to DHS-OIG, he worked at the U.S. Postal Service Office of Inspector General (USPS-OIG). At both agencies, Edwards had access to software systems, including one used for case management and other systems holding sensitive personal identifying information of employees.

After leaving DHS-OIG, Edwards founded Delta Business Solutions Inc., located in Maryland. From at least 2015 until 2017, he stole software from DHS-OIG, along with sensitive government databases containing personal identifying information of DHS and USPS employees, so that his company could develop a commercially-owned version of a case management system to be offered for sale to government agencies. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Navy Commander Pleads Guilty In Navy Bribery Scandal Involving 34 Navy Officials (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 over bill the Navy by over $35 million. (Source)

Former DoD Employee Pleads Guilty To Stealing Identities Of 37 Individuals In $240,000+ Bank / Loan Fraud Scheme 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)

Former Veterans Administration Employee Sentenced To Prison For Stealing Personal Protective Equipment & Other Medical Equipment, Then Selling - 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)

Former 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)

Former Pharmacy Executive Pleads Guilty To $88 Million Health Care Fraud Conspiracy Targeting Military Health Care Programs - January 26, 2022

Matthew Smith admitted his role in fraudulently billing Tricare and CHAMPVA for expensive, medically unnecessary compound drugs from a pharmacy. Tricare and CHAMPVA are the health care benefit programs for the United States Department of Defense and Department of Veterans Affairs.

Smith was the executive vice-president of the pharmacy. Smith and his co-conspirators paid approximately $40 million in kickbacks to patients, patient recruiters and doctors in exchange for their ordering expensive pain creams, scar creams and vitamins without regard to the beneficiaries' actual medical needs. The reimbursement rates sometimes reached $15,000 for a one-month supply.

In addition, the pharmacy did not charge beneficiaries the mandatory co-payments, something that the co-conspirators concealed. The fraudulent billings caused a loss to the programs of approximately $88 million. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS / UNIVERSITIES

Former City Of New Orleans Building Inspector Sentenced To Prison For Accepting $65,000 In Bribes - January 18, 2022

Kevon Richardson employed as a building inspector for the City of New Orleans.

He utilized the internet-based City of New Orleans' LAMA system to alter and / or delete city documents and submit material information. He solicited and accepted approximately $65,000 in bribe payments from individuals seeking favorable inspection reports and certificates of completion for properties that did not comply with the city and state building codes and for properties that had not been inspected. He also paid bribe money to a City of New Orleans permit analyst for the issuance of permits without proper documentation and plan review. (Source)

Former Chief Financial Officer For City Charged With Embezzling $760,000+ Of City Funds For Personal Gain - January 26, 2022

Tracy Hudson embezzled more than $762,000 from the City of Bardstown, Kentucky, while employed first as the City's Occupational Tax Administrator and then as its Chief Financial Officer.

Between 2013 and September 2019, Hudson stole funds from the City of Bardstown by various means, including by taking cash from the City of Bardstown funds for her own personal use, paying herself for false expense reimbursements, diverting additional payments into her 401k pension plan in excess of the amount withheld from her wages, purchasing personal items on a City of Bardstown credit card without authorization, and crediting payments to her personal accounts with the City of Bardstown despite no actual payment having been made. (Source)

Former Public Schools Employee Pleads Guilty To Defrauding School District Of $550,000+ Using Shell Company Fraud Scheme - January 27, 2022

David Marshall was a former media communications specialist employed by the Orangeburg County School District.

He, created a scheme to defraud the district while purchasing remote learning cameras for school classrooms. Through the use of shell companies, fabricated documents, forged signatures, and a false identity, Marshall steered the district's purchasing contracts to companies he created and controlled, purchased the cameras, then sold them to the school at a substantial markup.

Marshall also received funds from the school district for the cameras that he never paid to the seller. Through his scheme to defraud, Marshall received more than $550,000 in illegal proceeds. His scheme was eventually discovered by other school district employees, who confronted Marshall and reported the matter to the FBI for further investigation. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

2 Former Paramedics Posed As Nurses To Steal Morphine & Painkillers From Terminally Ill Individuals - January 12, 2022

Ruth Lambert and Jessica Silvester preyed on individuals receiving end-of-life care posing as nurses to achieve entry to their properties to steal the treatment.

Lambert and Silvester would communicate using WhatsApp messages figuring out victims after which go to and steal from. A probe discovered that they'd carried out as much as 29 burglaries.

Most of the victims weren't conscious of any wrongdoing till the police arrived and made enquiries, piecing collectively the offences with the help of subsequent of kin and victims. (Source)

Fort Lauderdale Police Officer Arrested For Fraudulently Billing Work Hours - January 13, 2022

A Fort Lauderdale police officer was arrested after an investigation revealed he fraudulently billed work hours. James McDowel turned himself in to the Broward County Main Jail to face three counts of grand theft and one count of organized scheme to defraud.

Preliminary details from the investigation have revealed several instances where McDowell signed on to work off-duty details while still working his regularly scheduled shift at the Fort Lauderdale Police Department. This resulted in several hundred fraudulently billed hours and the loss of thousands of dollars. (Source)

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

CEO Of Various Medical Imaging Companies Sentenced To Prison For $250 Million Health Care Fraud Scheme / Paid $9 Million In Kickbacks To Physicians - January 28, 2022

Sam Solakyan is the CEO of several Southern California medical imaging companies. He ran a scheme that submitted more than $250 million in fraudulent claims through the California Workers' Compensation System for medical services procured through bribes and kickbacks to physicians and others.

Solakyan paid some $9 million in kickbacks in order to generate over $250 million in fraudulent medical billings, the vast majority of which were for MRIs that were medically unnecessary. Solakyan devised, and through his kickbacks fueled, a cross-referral scheme that incentivized (co-conspirators)] to herd patients to physicians who over prescribed ancillary services in exchange for cash and other economic benefits."

From 2013 to November 2016, Solakyan conspired with physicians and others to perpetrate a scheme in which physicians were paid bribes and kickbacks in exchange for the referral of workers' compensation patients. The compensation offered to the corrupt doctors consisted of either cash or referrals of new patients. (Source)

3 Former GlaxoSmithKline Scientist Pleads Guilty To Stealing Trade Secrets To Benefit Chinese Pharmaceutical Company - January 3, 2022

Lucy Xi's, Yu Xue, Tao Li and Yan Mei, established a company named Renopharma. The company was supposedly to research and develop anti-cancer drugs. In reality, though, the company was used as a repository of information stolen from GlaxoSmithKline to benefit a Chinese pharmaceutical company named Renopharma.

Renopharma received financial support and subsidies from the government of China. At the time, Lucy Xi (Who Was Married To Yan Mei) and Yu Xue were employed as a scientists at a GSK facility in Upper Merion, PA, which worked on developing biopharmaceutical products. These products typically cost in excess of $1 billion to research and develop.

In January 2015, Lucy Xi sent Yan Mei a GSK document which contained confidential and trade secret data and information. The document provided a summary of GSK research into monoclonal antibodies at that time. In the body of the e-mail, Lucy Xi wrote, "You need to understand it very well. It will help you in your future business [RENOPHARMA]."

Yu Xue, her sister, Tian Xue, and Tao Li have all pleaded guilty for their roles in this conspiracy. Yan Mei is a fugitive who currently resides in China. (Source)

Former Nurse Working For Nursing Home Sentenced To Probation For Identity Theft / Credit Card Fraud Of Deceased Resident - January 3, 2022

A former nurse working at a Illinois nursing home was sentenced to 24 months of probation for identity theft. The nurse was accused of unlawful possession of a credit card and illegal drug possession.

A resident in the nursing home died on November 24, 2020. His daughter discovered that there were 21 transactions on her deceased father's credit card that occurred from the day of his death through December 2, 2020. Items that were charged to the resident's credit card after his death included a $405 utility bill; a video game for $299; and other fraudulent charges for food, gas, and a dog collar, totaling more than $1,700.

Video surveillance was viewed of several of the fraudulent transactions, and it showed the nurse making the transactions, sometimes still wearing her nursing scrubs. The nurse admitted to finding the deceased resident's credit card under a bedside table and using it to make the fraudulent purchases. (Source)

Suburban Chicago Nurse Charged With Tampering With Morphine Prescribed to Patients - January 13, 2022

A suburban Chicago nurse removed morphine from bottles prescribed to two patients and replaced it with another liquid, knowing the diluted substance would be dispensed to the patients.

Sarah Diamond was employed as the Assistant Director of Nursing at a Chicago-area medical rehabilitation center. The indictment alleges that Diamond tampered with the liquid morphine in August 2021 with reckless disregard and extreme indifference for the risk that the patients would be placed in danger of bodily injury. (Source)

University Of Arkansas Medical Sciences Notifying 518 Patients After Employee E-Mailed Protected Health Information To Her G-Mail Account - January 23, 2022

On Nov. 29, 2021, the University Of Arkansas Medical Sciences (UAMS) became aware that a former employee sent emails from her UAMS email to her personal Gmail account with patient information attached on November 15, 2021, while still employed with UAMS.

The attachments consisted of Excel spreadsheets used for internal billing compliance auditing purposes and / or billing statements addressed to UAMS for reimbursement. The information included the names of 518 patients, their hospital account numbers, dates of service, insurance type, claim information for billing purposes and medical record numbers. For a handful of patients, their dates of birth and medication information were also included. The former employee, who voluntarily left UAMS, contends it was a mistake. (Source)

Former Employee Of Toxicology Testing Laboratory Pleads Guilty To $14 Million+ Conspiracy Scheme Involving Co-Conspirators To Defraud North Carolina Medicaid Program - January 26, 2022

Richard Graves pleaded guilty to conspiracy to commit health care fraud and money laundering conspiracy for his role in a scheme to obtain more than $14 million from the North Carolina Medicaid program.

Graves was an employee of United Diagnostic Laboratories (UDL), a urine toxicology testing laboratory, and United Youth Care Services (UYCS), a company that provided mental health and substance abuse treatment services. From January 2016 to July 2020, Graves and his co-conspirators executed a conspiracy to defraud the North Carolina Medicaid program by paying illegal kickbacks to co-conspirators in exchange for urine samples from Medicaid-eligible beneficiaries.

Graves admitted in court that he and his co-conspirators located recruiters to recruit at-risk youths and other Medicaid-eligible beneficiaries for after-school, youth mentoring, housing, or other programs and services. Once enrolled, the beneficiaries were required to submit urine specimens for drug testing, which were provided to UDL and UYCS for medically unnecessary urine drug testing. Graves and his co-conspirators paid the recruiters a kickback from UYCS's NC Medicaid reimbursement on the drug testing.

In addition, Graves and his co-conspirators executed a conspiracy to launder the proceeds of the kickback and health care fraud conspiracy through Everlasting Vitality, a company owned by one of the recruiters. According to plea documents, Everlasting Vitality sent fraudulent invoices to UYCS listing the hours that the co-conspirators purportedly worked for UYCS in the prior month. The fraudulent invoices listed fake services that had not actually been provided to UYCS, including program development and design, community engagement, motivational speaking, and college mentorship services. In truth and in fact, the purpose of these invoices was to conceal and disguise the nature and source of UYCS's illegal kickback payments for drug testing referrals. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Employee (Chinese National) Pleads Guilty To Espionage / Trade Secret Conspiracy Against U.S. Company - January 6, 2022

Xiang Haitao was employed by Monsanto and its subsidiary, The Climate Corporation, from 2008 to 2017, where he worked as an imaging scientist.

Monsanto and The Climate Corporation developed a digital, online farming software platform that was used by farmers to collect, store and visualize critical agricultural field data and increase and improve agricultural productivity for farmers. A critical component to the platform was a proprietary predictive algorithm referred to as the Nutrient Optimizer. Monsanto and The Climate Corporation considered the Nutrient Optimizer a valuable trade secret and their intellectual property.

In June 2017, the day after leaving employment with Monsanto and The Climate Corporation, Xiang attempted to travel to China on a one-way airplane ticket. While he was waiting to board his flight, Federal officials conducted a search of Xiang's person and baggage. Investigators later determined that one of Xiang's electronic devices contained copies of the Nutrient Optimizer. Xiang continued on to China where he worked for the Chinese Academy of Science's Institute of Soil Science. Xiang was arrested when he returned to the United States. (Source)

BANKING / FINANCIAL INSTITUTIONS

Individual Pleads Guilty To Stealing $120,000+ From Wells Fargo Bank Customer Accounts With Help Of Bank Employees - January 6, 2022

Michael Drummond pleaded guilty today to a federal charge of conspiracy to commit bank fraud for his role in a scheme in which Wells Fargo Bank customers lost $124,000 from their accounts.

Drummond admitted to orchestrating a scheme that was carried out in 2017 in which Drummond recruited bank employees who would make unauthorized withdrawals from Wells Fargo customer accounts. The bank employees used the bank's internal systems to check the account balances of customers without the customer's knowledge. Those employees then told Drummond the customer's name and account balance.

Drummond then sent another accomplice into the bank to pose as the customer and to withdraw the funds, unbeknownst to the actual customer. The conspirators used this scheme to steal $124,000 in cash and an $80,000 cashier's check from two of the bank's customers. Although Wells Fargo was able to detect the theft and stop payment of the $80,000 cashier's check, Wells Fargo incurred losses on behalf of its customers for the $124,000 in cash that Drummond and others stole. (Source)

Former Bank Teller Sentenced To Prison For Embezzling $73,000 From Bank - January 7, 2022

Arin Kumhall was employed as a bank teller at a Citizens Bank in Westlake, Ohio. In addition to traditional teller responsibilities, Kumhall was responsible for ordering, receiving and inputting cash into the bank's internal reporting system for the branch.

On multiple occasions from September to December of 2020, Kumhall ordered a set amount of cash to be delivered to the branch. However, after the delivery, Kumhall entered and reported an amount lower than what had been delivered into the bank's internal reporting system. Kumhall pleaded guilty to embezzling nearly $73,000 from her employer. (Source)

Former Bank Loan Officer Sentenced To Prison For Obtaining $750,000+ Of Fraudulent Loans Over 10 Years - January 14, 2022

Jason McMillan admitted that from July 2009 through April 2019, he knowingly used the identity of another person without their consent in obtaining commercial loans in the amounts of $187,000, $160,000, $157,000 and $250,000 from a Chatham County bank where he worked as its commercial loan officer.

McMillan also admitted he obtained these loans under the false pretense that loans would be used for obtaining industrial farm equipment. McMillan admitted he knowingly used approximately $200,271 of these funds for his own personal use. The bank discovered the fraud during an internal investigation. (Source)

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

Former Business Manager For Health Care Agency Sentenced To Prison For Stealing $799,000+ - January 5, 2022

Alicia Raynor while working as the business manager for Compassion at Home, Inc., opened an account with Intuit, Inc., a payroll and payment processing service located outside the state of New York. She used the accounting software package Quickbooks to make payments into the Intuit account.

Raynor then diverted money from Compassion at Home's bank accounts to accounts that she controlled.

In order to avoid detection, Raynor disguised Quickbook entries to make it appear that the payments were to Bank of America, Capital One, or Compassion at Home employees. Raynor was ordered to pay restitution totaling $799,625.27. (Source)

Former Bookkeeper Admits To Embezzling $3.6 Million+ From Employer To Pay Credit Card Bills / Buy Properties - January 26, 2022

Trina Welch was employed by Kasco of Idaho, LLC as a bookkeeper from 2012 until July 3, 2019.

Beginning in at least 2013 and continuing until the day she was terminated on July 3, 2019, Welch used her position as a bookkeeper to engage in a scheme and plan to defraud Kasco and engage in a scheme to obtain money and property by making materially false and fraudulent representations and promises.

Welch embezzled funds from Kasco by writing and creating at least 341 checks which were drawn on the Kasco bank account. Those checks were written to Welch's own credit cards and money was applied to the credit cards outstanding balances. Welch admitted that in 2017 alone she took over $930,000 just to pay her Bank of America credit cards. Welch admitted she bought properties for herself and others related to her and spent the money at spas, travel for herself and family and friends, and other personal endeavors. Welch admitted that she took at least $1,500,000, and acknowledged that the United States contends she took at least $3,674,338.86 in total. (Source)

Former New Mexico Taxation And Revenue Employee Pleads Guilty To Wire Fraud, Identity Theft, Money Laundering Scheme To Enrich Himself With $689,000 - January 5, 2022

From May 18, 2011, through July 16, 2018, George Martinez allegedly used his position as the Unit Supervisor / Bureau Chief of the Questionable Refund Unit at the New Mexico Taxation and Revenue Department to fraudulently alter tax refunds and direct them to bank accounts that he controlled.

Martinez perpetrated the fraud by copying tax returns that had already been processed or creating new returns in taxpayers' accounts. He altered information such as taxpayers' Social Security numbers, bank account numbers and withholding amounts in the returns. By changing the withholding amounts, he increased the amounts of the refunds. Martinez fraudulently directed $689,797 into accounts in his control. (Source)

Former Bookkeeper For Accounting Firm Sentenced To Prison For $670,000 Fraud Scheme / Used Funds To Purchase Truck & Trailer - January 5, 2022

Paula Smith was a bookkeeper at an accounting firm that managed a lucrative trust account for a client (DEW. Trust). The DEW Trust, which was at one time valued at $8.6 million, had over twenty named beneficiaries, including twelve charitable organizations in St. Louis, Missouri.

Between October 2013 and June 2018, Smith defrauded the DEW Trust and its beneficiaries by writing numerous checks totaling $670,000 from the DEW Trust to herself. None of the funds should have gone to Smith.

To conceal her scheme, Smith manipulated the accounting records for the DEW Trust by mislabeling the fraudulent checks as being advance payments to a trustee and as payments to a vendor.

Smith used the funds to personally enrich herself, including to buy a 2017 Chevrolet Silverado K1500 and a 2018 Keystone Hornet Hideout 26RLS Travel Trailer. (Source)

Former Company Financial Controller Charged In $1.9 Million Dollar Fraud Scheme - January 5, 2022
Kerry Kit Yee Tang was employed as the controller of a San Francisco-based company that provides interior design services. Tang made unauthorized payments to herself and to outside companies from two of the victim company's bank accounts, embezzling a total of about $1.9 million.

From March 2019 to December 2020, Tang engaged in a scheme in which she obtained checks from her company's bank accounts and inserted "Kerry Tang" on the payee line. The indictment describes that Tang, without authorization to do so, signed the checks with the signatures of one or more of the authorized signers. Tang then deposited these checks into her own personal bank accounts. The indictment alleges that in this manner Tang obtained approximately 66 unauthorized checks from her company and deposited them to her personal bank accounts. The total amount of these deposits exceeded $1.6 million.

In November 2020 and December 2020 Tang wrote checks from a company bank account in amounts up to $99,000 to pay various companies for providing services to Tang's company. Tang signed each check with the signature of her company's authorized signers. However, Tang's company never engaged the services of these companies, and Tang was not authorized to write the checks. (Source)

Former Office Manager Sentenced To Prison For Stealing $200,000+ From Employer Over 9 Years To Pay Credit Card Debit - January 5, 2022
Raylene Vaillancourt worked as the office manager for a business. She was responsible for accounting and making payments to vendors.

Between at least April of 2009 and May of 2018, Vaillancourt embezzled money her employer through various means, including: (a) making fraudulent checks drawn on business checking account; (b) making unauthorized transfers to her personal financial accounts for her personal expenses; and (c) making unauthorized online payments from business checking account to pay her personal credit card debt.

As part of Vaillancourt's scheme, she altered businesses internal accounting records to conceal her embezzlement from her employer. In total, Business A lost approximately $200,000 due to the defendant's scheme. (Source)

Former Employee Sentenced To Prison For Defrauding Employer Of $4 Million+ To Purchase Cadillac, Designer Clothing, Luxury Watches, Etc. - January 6, 2022
David Hudson was an employee of Cummins Bridgeway, LLC (CBL) and Cummins Inc. (Cummins), two companies operating in New Hudson, Michigan. Hudson worked for CBL from approximately 2003 through 2014, until it was acquired by Cummins.

While working at CBL, Hudson's job involved transferring funds to these profit-sharing entities in the normal course of business. As part of his job, Hudson had authority to write checks from the profit-sharing entities. As part of the scheme to defraud, Hudson would, under false pretenses, direct an employee under his supervision to transfer CBL funds, and later Cummins funds into one or more of the profit-sharing entities. Hudson would then, without authorization, write checks from the profit-sharing entities to himself.

Between approximately 2008 and 2017, Hudson's scheme resulted in the fraudulent transfer of over $4.5 million dollars. This money was spent by Hudson to support a lavish lifestyle. For example, Hudson used stolen funds to purchase a Cadillac, designer clothing, luxury watches, cigars, and rare wines. (Source)

Former Senior Finance Employee Of Trucking Company Embezzled Hundreds of Thousands Of Dollars Following The Owner's Death - January 6, 2022

From September 2019 to February 2021, Benjamin Padua abused his senior finance position with his employer, and used falsified documents and improper accounting entries to embezzle hundreds of thousands of dollars.

Padua admitted that following the trucking company owner's death in October 2019, Padua forged the owner's signature on a fake employment agreement Padua created and backdated to prior to the owner's death. The fraudulent employment agreement purported to increase Padua's compensation significantly through higher wages, bonuses, and life insurance benefits. As Padua admitted in court today, after he created the fake employment agreement, Padua received substantial compensation from the trucking company, to which he was not entitled. (Source)

Bookkeeper Sentenced To Prison For Stealing $500,000+ From Former Employer To Pay For Personal Expenses - January 10, 2022

Before attending medical school, Walter Sytnik worked for a medical practice in southern New Jersey as a bookkeeper.

While employed by the practice, Sytnik stole some of its checks and, from May 2013 through April 2018, used them to steal more than $500,000 from the practice. He opened and maintained credit card accounts at the same banks as used by the doctor at the medical practice, and forged the doctor's signature on the stolen checks, which he sent through the U.S. Mail to pay his own credit card bills. When Sytnik ran out of checks, he reordered new ones so that he could continue the fraud. He used the stolen checks to pay personal expenses. (Source)

Former Financial Controller Sentenced To Prison For Embezzling $400,00+ From Family-Owned Business - January 10, 2022

Derick Cameron was sentenced to prison for embezzling more than $400,000 when he was employed as the Financial Controller for San Diego-based RAL Investment Corporation.

Cameron admitted that he abused his access to the company's accounting software by issuing more than 200 unauthorized checks to himself using the electronic signature of the company's CFO and depositing them into his personal bank account. He then concealed the payments by manipulating the company's accounting records to make it appear that each check was issued to a legitimate third-party vendor for a business expense. The company discovered Cameron's fraudulent activity in April 2018, fired Cameron, and reported the conduct to law enforcement when Cameron was unable to make his promised repayments on schedule. (Source)

Former Chief Executive Officer Pleads Guilty To Embezzling $15 Million+ Over 7 Years To Fund Extravagant Lifestyle - January 12, 2022

From at least 2013 to January 2020, Donna Steele, executed an extensive scheme to defraud her employer. Steele embezzled over $15 million from the company and used the money to support a business run by her and her family and to fund an extravagant lifestyle.

Steele was employed by the company from 1999 to January 2020. Initially, Steele worked in the shipping department and was promoted over the next 20 years to various positions within the company, including to the position of Chief Executive Officer (CEO), which she held until she was terminated in January 2020.

While serving as Vice President and later as CEO, Steele used her positions to embezzle funds from the company in a number of ways, including through fraudulent company credit card purchases, company checks, Quickbooks transactions, and wire transfers. Steele used company credit cards to pay for $6 million in personal expenditures, including to make high-end retail store purchases, to pay for luxury hotel accommodations and event ticket purchases, to buy expensive jewelry, to pay for family weddings, and to make purchases related to Opulence by Steele, a luxury clothing and boutique company the defendant founded in 2013.

In addition to the credit card purchases, Steele admitted to issuing and causing to be issued to herself approximately 98 checks totaling more than $2.8 million from the company's bank accounts, which Steele deposited into her personal bank account. Steele caused 127 fraudulent and unauthorized wire transfers to be executed as Quickbooks transactions, transferring more than $4.7 million from the company's bank accounts to her personal bank account. Steele executed at least 117 fraudulent and unauthorized bank wires, totaling more than $2.2 million, from the company's bank accounts to her personal bank account, which she then used for her personal benefit, including to fund a personal real estate closing. (Source)

Former Treasurer For County Agricultural Society Pleads Guilty To $100,000 Of Fraud Over 6 Years To Pay For Personal Expenses - January 14. 2022

Billy Harris admitted that from June 5, 2012 through October 3, 2018, he defrauded the Perry County Agricultural Society (PCAS) out of more than $100,000.

Harris paid his personal expenses, and purchased items for his personal use, with electronic debits from the PCAS bank account. Many of those items were purchased through Amazon. Some of the items that Harris admitted purchasing with PCAS funds include a WiFi router, Apple AirPods, a Himalyan Salt Lamp Air Purifier, Star Wars Darth Vader and Yoda personalized pet tags, a pair of Star Wars men's sleep pants, a floating pool fountain, a CPAP tube cleaning brush, and men's grooming products, including beard lube.

Harris also admitted writing checks on the PCAS account payable to himself and his spouse, and forging a Board member's signature on those checks. (Source)

Former Executive Vice President Charged With Embezzling $3.7 Million+ From National Cancer Research Organization - January 18, 2022

Melissa Goodwin embezzled over $3.7 million from the T.J. Martell Foundation for Cancer Research. The T.J. Martell Foundation is the music industry's leading foundation that funds innovative medical research focused on finding treatments and cures for cancer. Goodwin had been employed at the Foundation since 2005 and was the Executive Vice President and General Manager of the Foundation from 2018 until July 2020.

Between July 2018 and June 2020, Goodwin devised a scheme to defraud the T.J. Martell Foundation by purchasing approximately $3.96 million in tickets from online ticket vendors Ticketmaster, Stubhub, Primesport, and On-Location, using a Foundation credit card she had obtained in her own name. These tickets were not for a legitimate Foundation purpose and included tickets to musical concerts such as Lady Gaga and Celine Dion, and some were to sporting events, such as Super Bowl LIV, which was scheduled to take place in Miami, Florida, on February 2, 2020.

Goodwin provided these tickets to an individual in New York City who owned and operated a charity auction business. This business conducted auctions for clients, offering consignment items such as event tickets and sports memorabilia to the clients for use in their auctions. As part of the scheme, Goodwin led this individual to believe that she had acquired the tickets at no cost or at a discounted rate.

Goodwin also used the Foundation's credit card to purchase other items that were not for legitimate Foundation purposes, such as expensive and rare alcohols, plane tickets, and hotel stays. She then used the Foundation's bank accounts to pay the credit card charges.

In order to conceal the ticket purchases, Goodwin provided falsified credit card statements and false expense reports to the Foundation's accounting firm. Goodwin falsified the credit card statements by altering them to conceal the ticket purchases, as well as other expenses. She often replaced the name of the actual vendor with the name of a different vendor so that the charges appeared to be legitimate Foundation expenses. In total, Goodwin concealed over $3 million in fraudulent credit card expenses. (Source)

Detroit City Councilman Sentenced To Prison For Accepting $35,000+ In Bribes - January 19, 2022

While serving as an elected member of the Detroit City Council, Andre Spivey accepted $35,900 from an undercover federal law enforcement officer and a confidential source of information for the FBI.

On eight separate occasions between February 2018 and February 2020, Spivey, or a member of his staff identified as Public Official A, accepted bribe payments amounting to thousands of dollars from the undercover agent or the confidential source, all in connection with towing issues pending before the City Council.

Spivey served on the Detroit City Council from 2009 until September 2021, when he resigned from office immediately after pleading guilty in this case. (Source)

Former Employee For Children's Charity Sentenced To Prison For Stealing $4.7 Million+ In Federal Funds For Personal Use - January 24, 2022

Ruth Phillips worked at River Valley Child Development Services (RVCDS) from December 1986 until September 2020. She held various positions at the non-profit organization. Phillips served as Director of Business and Finance and was responsible for all financial operations, including monitoring accounts receivable, creating and submitting invoices, reconciling bank accounts and issuing checks.

From July 2016, to June 2017 RVCDS received approximately $7,131,756 in federal funding. Phillips stole approximately $964,012 during that period. Phillips further admitted that between December 2013 and August 2020, she stole approximately $4,721,731 from RVCDS.

During that period, she sent $1,142,500 to her personal checking account and sent another $3,395,500 to Attitude Aviation's bank account. Attitude Aviation has offices at Lawrence County Airpark in South Point, Ohio, and Tri-State Airport in Huntington and provides aeronautical services, including fueling, rental of hangar space, aircraft rental, flight instruction and maintenance. (Source)

Former UBS Financial Advisor Charged With Defrauding $5 Million+ From His UBS Clients Over 6 Years - January 24, 2022

From about 2012, and continuing to 2020, German Nino was a financial advisor working at a branch office of UBS Financial Services Inc. in Miami. Nino oversaw and managed UBS investment accounts for various customers, including three victims who were related and who had various investment accounts at UBS.

From about May 2014 to February 2020, Nino made a total of 62 unauthorized transfers from three UBS accounts belonging to the victims, which totaled $5,833,218.59.

To accomplish the wire fraud scheme, Nino made materially false and fraudulent statements to his victims and concealed and omitted material facts including misrepresenting the true performance, balance, and rate of return of the accounts he managed.

Nino forged the signature of his clients on documents purporting to authorize transfers out of the accounts; preparing a fraudulent land purchase contract and forging a victim's signature on the land purchase contract to make it appear that the victim was purchasing land in Colombia by using money from the victim's account, Nino removed one of the victim's email from the victim's UBS email account profile so that the victim would not receive email notifications from UBS about unauthorized transfers; and preparing fraudulent UBS account statements and client review statements, which falsely inflated the balance and value of the victims' accounts. (Source)

Former Bookkeeper Sentenced To Prison For Stealing $1.6 Million Over 8 Years To Support Husband's Lighting Business - January 26, 2022

Irene Scott is a former bookkeeper and financial manager for a private law firm in San Antonio. Scott worked for the law firm between August 2011 and February 2020. Her duties included issuing business credit cards to employees and closing those credit card accounts when an employee separated from the firm. She also maintained the firm's financial ledgers and paid vendors and operating expenses.

Scott pleaded guilty to three counts of wire fraud and one count of bank fraud. Scott admitted that from 2012 to 2020, she used three office credit cards assigned to other employees to make non-firm related purchases totaling over $1.2 million. An estimated three-fourths of those funds went to support her husband's outdoor lighting business. She concealed on the firm's financial ledgers credit card payments she made using the firm's operating account. Scott also stole an estimated $417,000 by fraudulently withdrawing from the firm's operating account about 200 times during a two-year period beginning in January 2018. She disguised those withdrawals in the firm's ledger as vendor payments. (Source)

Repeat Embezzler / Account Sentenced To Prison For Stealing Nearly $300,000 From Employer Over 7 Years For Personal use - January 28, 2022

Judith Wright worked as a contract accountant. Over 7 years, Wright stole nearly $300,000 from Transportation Demand Management LLC, a Washington State passenger transportation company. This is Wrights second conviction for embezzling. In 1994 she was sentenced to a year and a day in prison for embezzling from the bank where she served as Chief Financial Officer.

Between February 2010 and January 2017, Wright wrote some 120 fraudulent checks to herself and then disguised the payments in company books as if they were made to legitimate vendors. The fraud came to light when a new Chief Financial Officer at the company began questioning some of the entries. An FBI analysis of the accounts revealed that much of the money was clearly used for non-business expenses such as more than $78,000 in payments to Nordstrom, more than $17,000 spent with QVC, and more than $20,000 spent at Costco. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Former Bookkeeper Sentenced To Prison For $3.3 Million+ Fraud Scheme With Help Of Treasurer - January 12, 2022

Karen Duhon worked as the bookkeeper at Capital Management Consultants, Inc. (CMCI), a family-owned company located in Morgan City, Louisiana from October 1973 until August 2014.

From approximately January 1999, Duhon took money from CMCI unlawfully. With the assistance of the treasurer of CMCI at the time, Duhon began writing checks to herself in amounts over her allowed salary, which the treasurer would then sign. Duhon deposited the checks in various accounts owned by her and her husband. She would then make false accounting entries in CMCI's records to disguise these payments. The amount of loss suffered by CMCI was $3,263,677.06.

In addition, Duhon, along with the treasurer, also assisted certain members of the company owner's family with their personal finances, including paying bills and balancing accounts. This gave Duhon access to checks connected to a specific brokerage account owned by one of the family members. From November 2012 through January 2014, Duhon, with the aid and encouragement of the treasurer, and without authorization of the victim family member, used this brokerage account to pay $127,920.94 in expenses on her personal American Express cards. Further, in December 2013, Duhon, acting with intent to defraud, mailed or caused to be mailed to American Express a check in the amount of $8,370.03 drawn on the victim family member's account. (Source)

13 Individuals (NYPD Police Officer, Doctors, Attorney, Others) Charged In $100 Million Healthcare Fraud, Money Laundering, And Bribery Scheme in One of the Largest No-Fault Automobile Insurance Fraud Takedowns in History - January 12, 2022

Of the 13 defendants, 8 are charged in an indictment detailing conspiracies to commit healthcare fraud, money laundering, bribery, and obstruction, making false statements to federal authorities, and aggravated identity theft.

The 13 defendants charged in today's indictments are alleged to have collectively perpetrated one of the largest no-fault insurance frauds in history. In carrying out their massive scheme, among other methods, they allegedly bribed 911 operators, hospital employees, and others for confidential motor vehicle accident victim information. With this information, they then endangered victims by subjecting them to unnecessary and often painful medical procedures, in order to fraudulently over bill insurance companies. (Source)

Father And Son Plead Guilty To Charge Of Conspiracy To Defraud Their Former Employer Out Of $1.5 Million+ Over 8 Years - January 18, 2022

Anthony Montanelli and his father Steven Montanelli worked as biomedical engineers at Kaiser Foundation Hospitals and Health Plan, Inc. (Kaiser). They were responsible for repairing and servicing Kaiser ultrasound systems used at its medical facilities. The father and son used their positions at Kaiser to order new ultrasound parts that were supposed to be used to repair, replace, and / or maintain Kaiser's medical equipment, but instead were diverted to their own business, Pacific Coast Imaging (PCI). They then sold the diverted equipment through PCI for their own profit. The father and son also admitted operating their scheme and business, which they did not disclose to Kaiser, while being paid by Kaiser to service Kaiser-owned equipment.

Beginning February 2010 and continuing through about April 2018, they father and son worked together to defraud Kaiser. They rented storage units in which they stockpiled new, used, and decommissioned Kaiser-owned ultrasound systems and parts. Some of the Kaiser inventory they ordered through Kaiser became PCI inventory, which they sold and leased to PCI customers. The father and son acknowledged that for years they caused Kaiser's procurement specialists to process, order, and have mailed to them an unknown number of ultrasound parts which they diverted to PCI.

The loss to Kaiser resulting from the conspiracy exceeded $1,500,000. (Source)

THEFT OF COMPANY PROPERTY

Amazon Employee Pleads Guilty To Mail Fraud For Stealing More Than $273,000 In Merchandise & Reselling - January 28, 2022

From June 2020 to September 2021, Douglas Wright executed a scheme to defraud Amazon by stealing merchandise worth over $273,000 from the company's warehouse.

Over the course of the scheme, Wright was employed as an Operation's Manager at Amazon's warehouse. Wright misused his access to the company's computers to target certain merchandise, particularly computer parts such as internal hard drives, processors, and graphic processing units, and shipped those items from the warehouse to his home address. Wright admitted he the sold the stolen merchandise for profit to a computer wholesale company in California. (Source)

OTHER FORMS OF INSIDER THREATS

FBI WARNING: THE FBI HAS WARNED OF AN ATTACK CAMPAIGN THAT SENDS USB DRIVES CONTAINING MALICIOUS SOFTWARE TO EMPLOYEES

In January 2022, the FBI issued a public warning over a USB attack campaign in which numerous USB drives, laced with malicious software, were sent to employees at organizations in the transportation, defense, and insurance sectors between August and November 2021.

The USBs came with fake letters impersonating the Department of Health and Human Services and Amazon, sent via the U.S. Postal Service and UPS. The campaign has been dubbed BadUSB, and the FIN7 hacker organization has been named as the culprit. Here is what you need to know about BadUSB and mitigating the risks of this USB attack.

BadUSB Overview

"The BadUSB attack provides the victim with what looks like a physical USB stick and a lure to plug it into the victim's system, such as promising a gift card as a thank you or invoices that need to be processed," explains Karl Sigler, senior security research manager at Trustwave SpiderLabs. His malware research team initially discovered the campaign in 2020 while examining a malicious thumb drive as part of a forensic investigation for a U.S. hospitality provider.

The USB drive is actually configured as a USB keyboard, and the computer will identify it and configure it as such," he tells CSO. "Once inserted, the USB keyboard will automatically start typing and will typically invoke a command shell and inject commands to download malware." BadUSB, when successful, acts as an initial downloader for anything from credential grabbers to backdoors and ransomware.
(Source -1)
(Source -2)

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, 300+ 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 **650+** 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]